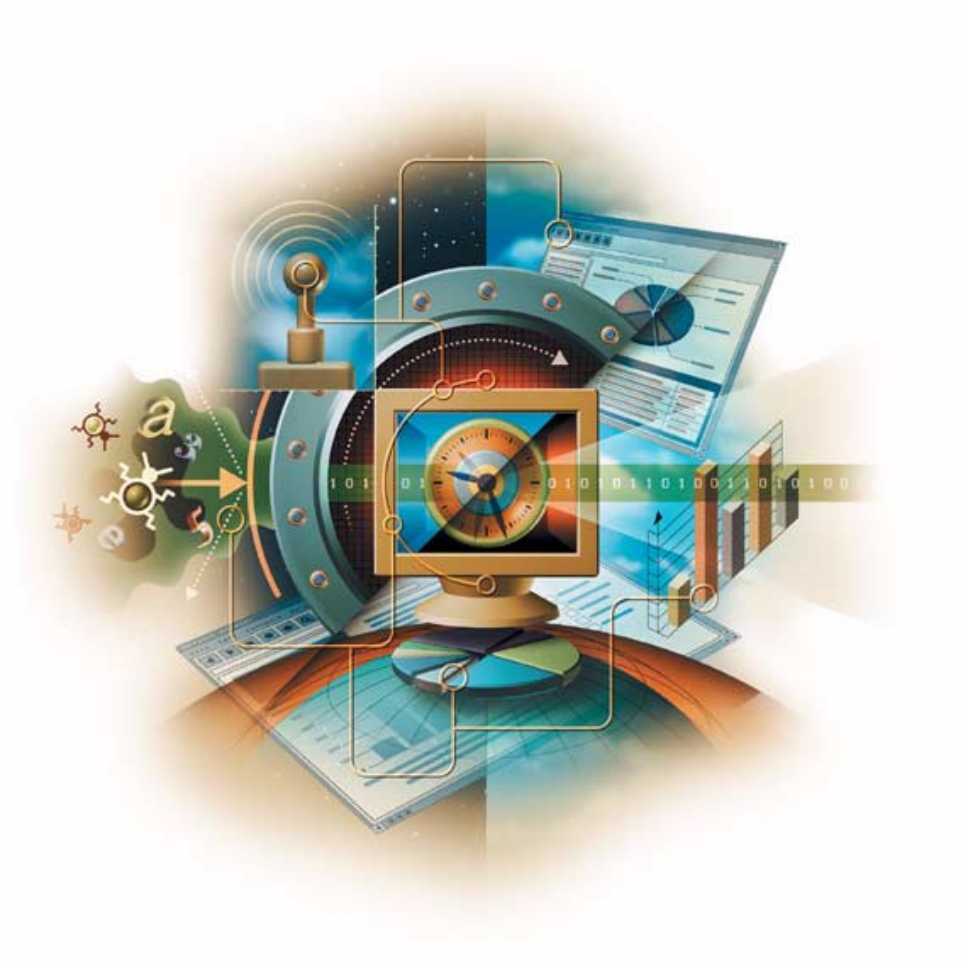
Produkthandbuch
Revision 1.0

VirusScan® Enterprise

Version 7.1.0



McAfee® SECURITY

COPYRIGHT

© 2003 Networks Associates Technology, Inc. Alle Rechte vorbehalten. Diese Veröffentlichung darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung der Network Associates Technology, Inc. oder ihrer Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden. Diese Genehmigung können Sie schriftlich bei der Rechtsabteilung von Network Associates unter der folgenden Adresse beantragen: 5000 Headquarters Drive, Plano, Texas 75024, USA; oder rufen Sie an unter +1-972-963-8000.

MARKEN

Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware und Design, Appera, AVERT, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, ClickNet, CNX, CNX Certification Certified Network Expert und Design, Covert, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomons Label, E und Design, Entercept, Enterprise SecureCast, Enterprise SecureCast (in Katakana), ePolicy Orchestrator, Event Orchestrator (in Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HelpDesk IQ, HomeGuard, Hunter, Impermia, InfiniStream, Intrusion Prevention Through Innovation, IntruShield, IntruVert Networks, LANGuru, LANGuru (in Katakana), M und Design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee und Design, McAfee.com, MultiMedia Cloaking, NA Network Associates, Net Tools, Net Tools (in Katakana), NetAsyste, NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, Network Performance Orchestrator, Network Policy Orchestrator, NetXray, NotesGuard, nPO, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PortalShield, Powered by SpamAssassin, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, Remote Desktop, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, SecureSelect, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SpamKiller, SpamAssassin, Stalker, SupportMagic, ThreatScan, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, VIDS, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, What's The State Of Your IDS?, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager sind eingetragene Marken der Network Associates, Inc. bzw. der angeschlossenen Tochterunternehmen in den USA und/oder anderen Ländern. Produkte der Marke Sniffer® werden ausschließlich von der Network Associates, Inc. hergestellt. Alle weiteren in diesem Dokument aufgeführten Marken sind geschützte Marken ihrer jeweiligen Inhaber.

LIZENZINFORMATIONEN

Lizenzvertrag

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN FÜR SIE GELTENDEN LIZENZVERTRAG GRÜNDLICH DURCH. DIESER VERTRAG ENTHÄLT DIE ALLGEMEINEN BEDINGUNGEN UND BESTIMMUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN IHNEN NICHT BEKANNT IST, WELCHEN LIZENZTYP SIE ERWORBEN HABEN, LESEN SIE DIES IM VERKAUFSBELEG ODER IN ANDEREN ZUGEHÖRIGEN LIZENZ- ODER BESTELLDOKUMENTEN NACH, DIE SIE ZUSAMMEN MIT IHREM SOFTWARE-PAKET ODER SEPARAT IM RAHMEN DES KAUFES ERHALTEN HABEN (Z. B. EINE BROSCHÜRE, EINE DATEI AUF DER PRODUKT-CD ODER EINE DATEI AUF DER WEBSITE, AUF DER SIE DIE SOFTWARE HERUNTERGELADEN HABEN). INSTALLIEREN SIE DIE SOFTWARE NICHT, WENN SIE NICHT ALLEN IM VERTRAG ENTHALTENEN BESTIMMUNGEN ZUSTIMMEN. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN NETWORK ASSOCIATES ODER DIE VERKAUFSSTELLE ZURÜCKGEBEN.

Zuordnungen

Dieses Produkt enthält bzw. kann enthalten:

- Software, die vom OpenSSL-Projekt für die Verwendung im OpenSSL-Toolkit (http://www.openssl.org/) entwickelt wurde.
- Kryptographie-Software von Eric Young (eay@cryptsoft.com) und Software von Tim J. Hudson (tjh@cryptsoft.com).
- Softwareprogramme, für die der Benutzer über eine Lizenz (oder Unterlizenz) gemäß der GNU General Public License (GPL) oder andere Free Software-Lizenzen verfügt, die den Benutzer unter anderem dazu berechtigen, bestimmte Programme oder Teile davon zu kopieren, zu bearbeiten oder weiterzuverbreiten und auf den Quellcode zuzugreifen. Die GPL schreibt vor, dass bei sämtlicher unter die GPL fallenden Software, die an eine Person in einem ausführbaren Binärformat weitergegeben wird, diesem Benutzer auch der Quellcode zugänglich gemacht werden muss. Bei sämtlicher Software, die unter die GPL fällt, ist der Quellcode ebenfalls auf dieser CD verfügbar. Wenn bestimmte Free Software-Lizenzen vorschreiben, dass Network Associates Rechte zum Verwenden, Kopieren oder Bearbeiten eines Softwareprogramms vergibt, die umfangreicher sind als die in dieser Vereinbarung gewährten Rechte, haben diese Rechte Vorrang gegenüber den Rechten und Einschränkungen in dieser Vereinbarung.
- Software, ursprünglich geschrieben von Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer.
- Software, ursprünglich geschrieben von Robert Nordier, Copyright © 1996-7 Robert Nordier. Alle Rechte vorbehalten.
- Software von Douglas W. Sauder.
- Software, entwickelt von der Apache Software Foundation (http://www.apache.org/).
- International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation und andere. Alle Rechte vorbehalten.
- Software. Entwickelt von CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc.
- FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Germany.

Inhalts

Vorwort 9

Die Zielgruppe 9
Konventionen 10
Informationsquellen 11
Kontaktaufnahme mit McAfee Security und Network Associates 12

1 Einführung zu VirusScan Enterprise 15

Verbesserungen und neue Funktionen 16
Produktkomponenten 17

2 Erste Schritte 21

Orientierung auf die Benutzeroberfläche 22
Startmenü 22
VirusScan-Konsole 23
Menüleiste 24
Menü "Task" 24
Menü "Bearbeiten" 25
Menü "Ansicht" 25
Menü "Extras" 25
Menü "Hilfe" 26
Symbolleiste 26
Taskliste 27
Statusleiste 28
Kontextmenüs 28
Kontextmenüs in der Konsole 29
Scannen über rechte Maustaste 30
Systemablage 30
Scannen oder Aktualisieren über das Kontextmenü der Systemablage 30
Befehlszeile 32
Einrichten von Benutzeroberflächenoptionen 32
Anzeigeoptionen 33
Kennwortoptionen 34
Entsperren und Sperren der Benutzeroberfläche 37

Einrichten von Scan-Vorgängen 38
Scannen bei Zugriff im Vergleich zum Scannen auf Anforderung 38
Automatisches Scannen 39
Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten . . . 40
Virusinformationsbibliothek 41
Einsenden eines Virenbeispiels 41
Einrichten der Remoteverwaltung 42

3 Scannen bei Zugriff 45

Konfigurieren des Zugriffsscanners 46
Eigenschaften des Scannens bei Zugriff 47
Allgemeine Einstellungen 49
Allgemeine Eigenschaften 49
Benachrichtigungseigenschaften 51
Berichtseigenschaften 53
Vorgangseinstellungen 56
Standardvorgänge 57
Vorgangseigenschaften 58
Erkennungseigenschaften 59
Erweiterte Eigenschaften 62
Aktionseigenschaften 64
Vorgänge mit geringem und hohem Risiko 67
Zuordnen eines Risikos zu einem Vorgang 67
Vorgangseigenschaften 69
Erkennungseigenschaften 72
Hinzufügen von Dateityperweiterungen 75
Hinzufügen benutzerdefinierter Dateityperweiterungen 76
Ausschließen von Dateien, Ordnern und Laufwerken 78
Erweiterte Eigenschaften 81
Aktionseigenschaften 84
Anzeigen von Scan-Ergebnissen 87
Anzeigen von Scan-Statistiken 87
Anzeigen des Aktivitätsprotokolls 88
Reaktionen auf die Erkennung von Viren 89
Empfangen von Benachrichtigungen über die Erkennung von Viren 89
Anzeigen der Nachrichten vom Zugriffsscanner 91
Durchführen von Aktionen bei einer Viruserkennung 92

4 Scannen auf Anforderung 95

Erstellen von Anforderungstasks 96
Erstellen von Tasks mithilfe des Menüs "Start" oder der Systemablage 96
Erstellen von Tasks über die Konsole 98
Konfigurieren von Anforderungstasks 99
Ortseigenschaften 100
Hinzufügen, Entfernen und Bearbeiten von Elementen 101
Hinzufügen von Elementen 101
Entfernen von Elementen 103
Bearbeiten von Elementen 103
Erkennungseigenschaften 104
Erweiterte Eigenschaften 106
Aktionseigenschaften 110
Berichtseigenschaften 113
Zurücksetzen oder Speichern von Standardeinstellungen 115
Planen von Anforderungstasks 116
Scan-Vorgänge 117
Ausführen von Anforderungstasks 117
Unterbrechen und Neustarten von Anforderungstasks 119
Ausführen von Anforderungstasks 119
Fortsetzbare Scan-Vorgänge 119
Anzeigen von Scan-Ergebnissen 119
Anzeigen von Scan-Statistiken 120
Anzeigen des Aktivitätsprotokolls 121
Reaktionen auf die Erkennung von Viren 121
Empfangen von Benachrichtigungen über die Erkennung von Viren 122
Durchführen von Aktionen bei einer Viruserkennung 123
Dialogfeld "VirusScan-Warnung" 123
Dialogfeld "Status des Scannens auf Anforderung" 124

5 Scannen von E-Mails 127

E-Mail-Empfangsscan 128
Konfigurieren des E-Mail-Scans bei Empfang für einen lokalen oder Remote-Host 128
Anzeigen der Eigenschaften des E-Mail-Scans bei Empfang 129
Erkennungseigenschaften 129
Erweiterte Eigenschaften 131
Aktionseigenschaften 135
Warnungseigenschaften 138
Berichtseigenschaften 140
Anzeigen der Ergebnisse des E-Mail-Scans bei Empfang 142
Anzeigen der Statistik des E-Mail-Scans bei Empfang 143
Anzeigen des Protokolls für E-Mail-Aktivitäten bei Empfang 144
E-Mail-Scan auf Anforderung 144
Konfigurieren des E-Mail-Anforderungstasks 145
Erkennungseigenschaften 145
Erweiterte Eigenschaften 148
Aktionseigenschaften 151
Warnungseigenschaften 154
Berichtseigenschaften 156
Ausführen des E-Mail-Anforderungstasks 158
Anzeigen der Ergebnisse des E-Mail-Anforderungsscans 160
Anzeigen des Protokolls für E-Mail-Aktivitäten auf Anforderung 160

6 Virenwarnungen 161

Konfigurieren des Warnungs-Managers 162
Konfigurieren von Empfängern und Methoden 166
Überblick über das Hinzufügen von Warnmethoden 168
Senden einer Testnachricht 168
Einrichten der Warnungsprioritätsstufe für Empfänger 169
Anzeigen der Seite "Zusammenfassung" 170
Weiterleiten von Warnmeldungen an andere Computer 171
Senden von Warnungen als Netzwerkmeldungen 175
Senden von Warnmeldungen an E-Mail-Adressen 177
Senden von Warnmeldungen an einen Drucker 181
Senden von Warnmeldungen per SNMP 183
Starten eines Programms als Warnung 185

Protokollieren von Warnbenachrichtigungen im Ereignisprotokoll des Computers 186
Senden einer Netzwerkmeldung an einen Terminalserver 188
Verwenden von zentralen Warnungen 190
Anpassen von Warnmeldungen 192
Aktivieren und Deaktivieren von Warnmeldungen 193
Bearbeiten von Warnmeldungen 194
Ändern der Warnpriorität 194
Bearbeiten des Warnmeldungstexts 196
Verwenden von Systemvariablen des Warnungs-Managers 196

7 Aktualisieren 199

Aktualisierungsstrategien 200
Systemvariablen 201
AutoUpdate-Tasks 202
Übersicht über die AutoUpdate-Tasks 203
Erstellen eines AutoUpdate-Tasks 204
Konfigurieren eines AutoUpdate-Tasks 204
Ausführen von AutoUpdate-Tasks 206
Ausführen von Aktualisierungs-Tasks 206
Aktivitäten während eines Aktualisierungs-Tasks 209
Anzeigen des Aktivitätsprotokolls 210
AutoUpdate-Repository-Liste 210
AutoUpdate-Repositories 211
Konfigurieren der AutoUpdate-Repository-Liste 211
Importieren der AutoUpdate-Repository-Liste 212
Bearbeiten der AutoUpdate-Repository-Liste 213
Hinzufügen und Bearbeiten von Repositories 213
Entfernen und Neuorganisieren von Repositories 220
Festlegen von Proxy-Einstellungen 221
Spiegelungstasks 224
Erstellen eines Spiegelungstasks 225
Konfigurieren eines Spiegelungstasks 226
Ausführen von Spiegelungstasks 228
Anzeigen des Aktivitätsprotokolls für Spiegelungstasks 230
Rollback für DAT-Dateien 230
Manuelle Aktualisierungen 232
Aktualisieren über DAT-Dateiarchive 233

8 Planen von Tasks 235

Task-Pläne konfigurieren 236
Task-Eigenschaften 237
Eigenschaften des Zeitplans 238
Planen der Häufigkeit von Tasks 239
Erweiterte Zeitplanoptionen 240
Planen von Tasks nach Häufigkeit 241
Täglich 241
Wöchentlich 243
Monatlich 244
Einmal 246
Bei Systemstart 248
Bei der Anmeldung 249
Bei Leerlauf 250
Sofort ausführen 251
Beim Einwählen ausführen 252

A Befehlszeilen-Scannerprogramm 253

VirusScan Enterprise -Befehlszeilenoptionen 253
Befehlszeilenargumente für das Scannen auf Anforderung 262
Anpassen der Installationseigenschaften 265

B Sichere Registrierung 269

Registrierungsschlüssel, für die Schreibzugriff erforderlich ist 270

C Fehlerbehebung 277

Minimum Escalation Tool 277
Häufig gestellte Fragen 277
Fragen zur Installation 278
Fragen zum Scannen 279
Fragen zu Viren 279
Allgemeine Fragen 281
Aktualisieren von Fehlercodes 284

Glossar 287

Index 301

Vorwort

Dieses Handbuch enthält eine Einführung in die McAfee® VirusScan® Enterprise-Software Version 7.1.0 und beschreibt die folgenden Themen:

- Überblick über das Produkt
- Beschreibung der Produktfeatures
- Beschreibung der neuen Funktionen in dieser Version der Software
- Detaillierte Anleitungen zur Konfiguration und Ausbringung der Software
- Verfahrensweisen zur Ausführung der Tasks
- Informationen zur Fehlerbehebung
- Glossar

Die Zielgruppe

Die Informationen in diesem Handbuch sind in erster Linie an zwei Zielgruppen gerichtet:

- Netzwerkadministratoren, die für das Virenschutz- und Sicherheitsprogramm ihres Unternehmens verantwortlich sind.
- Benutzer, die für die Aktualisierung der Virusdefinitionsdateien (DAT-Dateien) auf ihrem Computer oder für die Konfiguration der Erkennungsoptionen der Software verantwortlich sind.

Konventionen

In diesem Handbuch werden folgende Konventionen verwendet:

Fett

Begriffe aus der Benutzeroberfläche, unter anderem Namen von Optionen, Menüs, Schaltflächen und Dialogfeldern.

Beispiel
Geben Sie den **Benutzernamen** und das **Kennwort** des gewünschten Kontos ein.

`Courier`

Text, der für manuelle Benutzereingaben steht, beispielsweise Befehle an der Eingabeaufforderung.

Beispiel
Um den Agenten zu aktivieren, führen Sie an der Befehlszeile auf dem Client-Computer folgenden Befehl aus:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

Kursiv

Namen von Produkthandbüchern und Themen (Überschriften) in diesen Handbüchern; Hervorhebungen; neu eingeführte Begriffe.

Beispiel
Weitere Informationen finden Sie im *Produkthandbuch zu VirusScan Enterprise*.

<BEGRIFF>

Allgemeine Begriffe sind in spitze Klammern eingeschlossen.

Beispiel
Klicken Sie in der Konsolenstruktur unter **ePolicy Orchestrator** mit der rechten Maustaste auf <SERVER>.

HINWEIS

Ergänzende Informationen, beispielsweise eine alternative Methode für die Ausführung eines Befehls.

WARNUNG

Wichtiger Hinweis für den Schutz des Unternehmens oder den Schutz von Benutzern, Computersystemen, Software-Installationen oder Daten.

Informationsquellen

Installationshandbuch *†	Systemanforderungen sowie Anleitungen zur Installation und zum Starten der Software. *VirusScanEnterprise 7.1.0 Installationshandbuch*
Produkthandbuch *	Einführung und Funktionen des Produkts, detaillierte Anleitungen zur Konfiguration der Software, Informationen zur Ausbringung, sich wiederholende Aufgaben und Verfahrensabläufe. *VirusScanEnterprise 7.1.0 Produkthandbuch*
Hilfe §	Sehr hilfreiche und detaillierte Informationen zur Konfiguration und Verwendung der Software. Infothemen auf Feldebene (*Was ist das?*).
Konfigurationshandbuch *	*Zur Verwendung mit ePolicy Orchestrator™.* Verfahrensweisen für die Konfiguration, Ausbringung und Verwaltung Ihres McAfee Security-Produkts mithilfe der Verwaltungssoftware ePolicy Orchestrator.
Implementierungshandbuch *	Ergänzende Informationen zu Produktfeatures, Tools und Komponenten.
Versionshinweise ‡	*Readme.* Produktinformationen, behobene Fehler, bekannte Probleme sowie die jüngsten Ergänzungen oder Änderungen am Produkt oder der dazugehörigen Dokumentation.
Kontakte ‡	Kontaktinformationen für die Dienste und Ressourcen von McAfee Security und Network Associates: technischer Support, Kundendienst, AVERT (Anti-Virus Emergency Response Team), Beta-Programm und Schulungen. Diese Datei enthält außerdem Telefon- und Faxnummern sowie Post- und Web-Adressen der Niederlassungen von Network Associates in den Vereinigten Staaten und weltweit.

* Eine Adobe Acrobat PDF-Datei auf der Produkt-CD oder der Download-Site von McAfee Security.

† Ein gedrucktes Handbuch, das im Lieferumfang der Produkt-CD enthalten ist. Hinweis: Einige Sprachversionen des Handbuchs sind möglicherweise nur als .PDF-Datei verfügbar.

‡ Textdateien, die in der Software-Anwendung und auf der Produkt-CD enthalten sind.

§ Hilfe, die über die Software-Anwendung aufgerufen werden kann: Hilfemenü und/oder Hilfeschaltfläche für Hilfe auf Seitenebene; Option im Kontextmenü für Infothemen (*Was ist das?*).

Kontaktaufnahme mit McAfee Security und Network Associates

Technischer Support	
Homepage	http://www.networkassociates.com/us/support/
KnowledgeBase-Suche	https://knowledgemap.nai.com/phpclient/homepage.aspx
PrimeSupport- Service-Portal *	http://mysupport.nai.com
McAfee Security-Beta-Programm	http://www.networkassociates.com/us/downloads/beta/
Sicherheitshauptquartier – AVERT (Anti-Virus Emergency Response Team)	
Homepage	http://www.networkassociates.com/us/security/home.asp
Virusinformationsbibliothek	http://vil.nai.com
Übermitteln eines Beispiels – AVERT WebImmune	https://www.webimmune.net/default.asp
AVERT DAT-Benachrichtigungsdienst	http://www.networkassociates.com/us/downloads/updates/
Download-Site	
Homepage	http://www.networkassociates.com/us/downloads/
DAT-Datei- und Modulaktualisierungen	http://www.networkassociates.com/us/downloads/updates/ ftp://ftp.nai.com/pub/antivirus/datfiles/4.x
Produkt-Upgrades *	https://secure.nai.com/us/forms/downloads/upgrades/login.asp
Schulungen	
McAfee Security University	http://www.networkassociates.com/us/services/education/mcafee/university.htm
Network Associates-Kundendienst	
E-Mail	services_corporate_division@nai.com
Web	http://www.nai.com/us/index.asp http://www.networkassociates.com/us/products/mcafee_security_home.htm
USA, Kanada und Lateinamerika (gebührenfrei):	
Telefon	**+1-888-VIRUS NO** oder **+1-888-847-8766** Mo – Fr, 08.00 – 20.00 Uhr, Central Time

McAfee ist sehr daran interessiert, Ihr Feedback bei den Lösungsfindungen zu berücksichtigen. Wenn Sie linguistisches Feedback oder Kommentare zur verwendeten Sprache in den McAfee-Produkten haben, senden Sie uns eine E-Mail an: B2BLoc_DE@nai.com

Weitere Informationen zur Kontaktaufnahme mit Network Associates und McAfee Security (einschließlich gebührenfreier Nummern für andere Länder) finden Sie in der Kontakt-Datei, die im Lieferumfang dieses Produkts enthalten ist.

* Anmeldedaten erforderlich.

Einführung zu VirusScan Enterprise 1

Die Software VirusScanEnterprise 7.1.0 bietet Schutz gegen Viren sowohl für Server als auch für Arbeitsstationen. Die Software bietet leicht skalierbaren Schutz, schnelle Leistung und ein mobiles Design. Sie können lokale und Netzwerklaufwerke sowie E-Mail-Nachrichten und Anhänge für Microsoft Outlook scannen, die Anwendung so konfigurieren, dass sie immer bei Erkennung einer Infektion reagiert, und Berichte zu den Aktionen der Anwendung erstellen.

VirusScan Enterprise ersetzt folgende Softwareversionen:

- VirusScan Version 4.5.1 für Arbeitsstationen.
- NetShield ® NT Version 4.5 für Server.
- NetShield für Celerra™ Version 4.5 für Celerra™-Dateiserver.
- VirusScan Enterprise Version 7.0. für Workstations und Server.

In diesem Produkthandbuch werden die Konfiguration und die Verwendung der Software VirusScan Enterprise erläutert. Informationen zu den Systemanforderungen sowie Installationsanleitungen finden Sie im *VirusScan Enterprise-Installationshandbuch*.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Verbesserungen und neue Funktionen
- Produktkomponenten

Verbesserungen und neue Funktionen

Diese Version von VirusScan Enterprise enthält folgende Erweiterungen:

- **Integration mit Check Point™ VPN-1®/FireWall-1® SCV** – VirusScan Enterprise wurde für die Integration mit CheckPoint™ VPN-1/FireWall-1®SCV erweitert. Check Point kann nach der Installation und Aktivierung so konfiguriert werden, dass Clients ohne aktuellen Virenschutz nicht über das Virtual Private Network (VPN) auf das Unternehmensnetzwerk zugreifen können.

  Weitere Informationen über die Konfiguration von Check Point finden Sie im *VirusScanEnterprise 7.1.0 Installationshandbuch*.

- **Integration mit McAfee Installation Designer™ und McAfee Desktop Firewall™** – Mit McAfee Installation Designer können Sie McAfee Desktop Firewall mit VirusScanEnterprise 7.1.0 konfigurieren. Nach der Konfiguration können Sie beide Produkte gemeinsam bereitstellen und die Anzahl der erforderlichen Neustarts auf maximal einen reduzieren.

  Weitere Informationen finden Sie im *Produkthandbuch zu McAfee Installation Designer*.

- **Kleineres Installationspaket** – Das VirusScan Enterprise-Installationspaket wurde mithilfe der Netopsystems-Technologie Fast Electronic Application Distribution (FEAD® Optimizer®) optimiert. Dadurch reduziert sich die für Ausbringungen erforderliche Netzwerkbandbreite. Sie können McAfee Installation Designer 7.1 oder höher verwenden, um das Paket neu zusammenzustellen und dann das Paket erneut zu optimieren, nachdem Änderungen vorgenommen wurden. Bei der Ausführung von SETUP.EXE von der Befehlszeile aus können Sie spezielle Befehle und Optionen anwenden, um die Installationsdateien neu zusammenzustellen.

  Weitere Informationen über die Konfiguration des FEAD Optimizer von Netopsystems finden Sie im *VirusScanEnterprise 7.1.0 Installationshandbuch*.

- **Modul- und** DAT**-Dateien innerhalb der Datei .**MSI – Die Modul- und .DAT-Dateien wurden der .MSI-Datei für VirusScanEnterprise 7.1.0 hinzugefügt. So können Kunden das Produkt mit nur einer einzigen .MSI-Datei bereitstellen.

- **Sichtbarkeit von ePolicy Orchestrator-Tasks** – Wenn Sie ePolicy Orchestrator 3.0 oder höher zur Verwaltung der VirusScan Enterprise-Software verwenden, können Sie ePolicy Orchestrator-Tasks für Anforderungsscans, Aktualisierungen und Spiegelungen an der VirusScan-Konsole verwenden. Dadurch können die Endbenutzer alle Tasks sehen, die auf ihrem Computer ausgeführt werden, und Administratoren und Help Desk-Mitarbeitern wird die telefonische Fehlerbehebung bei ePolicy Orchestrator-Tasks erleichtert.

  Einzelheiten zur Aktivierung der Tasksichtbarkeit für ePolicy Orchestrator finden Sie im *VirusScanEnterprise 7.1.0-Konfigurationshandbuch für die Verwendung mit ePolicy Orchestrator 3.0*.

Produktkomponenten

VirusScan Enterprise besteht aus mehreren Komponenten, die als Features installiert sind. Jedes dieser Features spielt beim Schutz Ihres Computers gegen Viren oder potenziell unerwünschte Programme eine bestimmte Rolle. Folgende Features sind vorhanden:

- **VirusScan-Konsole**: Die Konsole ist die Steuerungszentrale, von der aus Sie VirusScan Enterprise-Tasks erstellen, konfigurieren und ausführen können. Als *Tasks* werden Vorgänge wie z. B. die Ausführung eines Scans auf mehreren Laufwerken und zu einem bestimmten Zeitpunkt bzw. innerhalb eines bestimmten Zeitraums oder die Ausführung einer Aktualisierung bezeichnet. Sie können den Zugriffsscanner an der Konsole aktivieren bzw. deaktivieren, sofern Sie über Administratorrechte verfügen, und falls erforderlich das entsprechende Kennwort eingeben.

  Siehe *VirusScan-Konsole* auf Seite 23.

- **Zugriffsscanner**: Der Zugriffsscanner gewährleistet einen dauerhaften Schutz vor Viren, die von Disketten, aus dem Netzwerk oder aus den verschiedensten Quellen im Internet stammen können. Der Scanner wird bei der Installation der Software vollständig konfiguriert; er wird beim Start des Computers gestartet und bleibt so lange im Arbeitsspeicher, bis der Computer heruntergefahren wird. Der Scanner bietet eine vorgangsbasierte Scan-Funktion, bei der die Scan-Richtlinien mit Anwendungen wie dem Internet Explorer verknüpft werden können. Auf verschiedenen Eigenschaftenseiten kann festgelegt werden, welche Teile des Systems vom Scanner geprüft werden sollen, worauf dabei geprüft wird, welche Teile von der Prüfung ausgeschlossen werden und wie auf infizierte Dateien reagiert werden soll, die der Scanner findet. Darüber hinaus kann der Scanner bei der Erkennung von Viren Warnungen ausgeben und Berichte erstellen, in denen die einzelnen Aktionen erfasst sind.

  Siehe *Scannen bei Zugriff* auf Seite 45.

- **Anforderungsscanner**: Mit dem Anforderungsscanner können Sie Scan-Vorgänge jederzeit starten. Dabei haben Sie die Möglichkeit, Scan-Ziele und auszuschließende Bereiche, die Reaktionsweise des Scanners bei der Virenerkennung und die Anzeige von Berichten festzulegen, in denen erkannte Viren und ausgegebene Warnungen erfasst werden. Darüber hinaus können Scan-Tasks erstellt werden, die zu einem bestimmten Zeitpunkt oder innerhalb eines angegebenen Zeitraums ausgeführt werden. Die Anzahl der verschiedenen auf Anforderung auszuführenden Scan-Tasks, die Sie definieren können, ist unbegrenzt und richtet sich ausschließlich nach Ihren Anforderungen. Konfigurierte Tasks können für die spätere Verwendung auch gespeichert werden.

  Siehe *Scannen auf Anforderung* auf Seite 95.

- **E-Mail-Scanner**: Mit dem E-Mail-Scanner können Sie Nachrichten und Anlagen in Microsoft Outlook sowie öffentliche Ordner, auf die Sie Zugriff haben, direkt auf dem Computer scannen. Wenn Outlook ausgeführt wird, werden die E-Mails beim Empfang gescannt. Darüber hinaus können E-Mails jederzeit auf Anforderung gescannt werden. Dadurch können Sie potenzielle Infektionen finden, bevor diese Ihren Desktop befallen.

  Siehe *Scannen von E-Mails* auf Seite 127.

- **AutoUpdate**: Mit dem Feature AutoUpdate werden die Virusdefinitionsdateien (DAT) und das Scan-Modul automatisch aktualisiert und die Aktualisierungen auf die Netzwerkcomputer verteilt. Darüber hinaus kann die Funktion zum Herunterladen von HotFix-Dateien verwendet werden. Je nach der Größe Ihres Netzwerks weisen Sie für das automatische Herunterladen der aktuellen Dateien von der HTTP-Site von Network Associates einen oder mehrere vertrauenswürdige Computer zu, von denen einer der Host Ihrer internen HTTP-Website ist.

  Siehe *Aktualisieren* auf Seite 199.

  HINWEIS
  AutoUpdate ist eine der Common Core (gemeinsames Framework) -Technologien, die von vielen Produkten verwendet werden.

- **Planer**. Mit diesem Feature können Sie Anforderungs-, Aktualisierungs- und Spiegelungstasks zu bestimmten Zeiten oder in Intervallen planen.

  Siehe *Planen von Tasks* auf Seite 235.

  HINWEIS
  Der Planer ist eine der Common Core (gemeinsames Framework) -Technologien, die von vielen Produkten verwendet werden.

- **Warnungs-Manager**: Der Warnungs-Manager™ ermöglicht Ihnen, Viruswarnungen zu empfangen oder zu senden. Nach der Installation können Sie den Warnungs-Manager so einrichten, dass bei Erkennung eines Virus auf dem Computer sofort eine Benachrichtigung per E-Mail, über einen Drucker, SNMP-Traps oder andere Wege an Sie gesendet wird. Der Warnungs-Manager ist standardmäßig nicht vorkonfiguriert, d. h. bevor Sie Virenwarnungen empfangen oder senden können, müssen Sie die Software entsprechend konfigurieren.

  Einzelheiten dazu finden Sie unter *Virenwarnungen* auf Seite 161.

- **Befehlszeilenscanner:** Der Befehlszeilenscanner kann eingesetzt werden, um im Dialogfeld Eingabeaufforderung zielgerichtete Scan-Vorgänge auszulösen. Der nur für Windows NT-Umgebungen konzipierte Scanner SCAN.EXE ist die wichtigste Befehlszeilenoberfläche.

Normalerweise wird für die Scan-Vorgänge die Benutzeroberfläche von VirusScan Enterprise verwendet. Wenn Sie jedoch Probleme mit dem Starten von Windows haben oder die Features von VirusScan Enterprise in Ihrer Umgebung nicht funktionieren, haben Sie immer noch die Möglichkeit, den Befehlszeilenscanner zu verwenden.

Siehe *Befehlszeilen-Scannerprogramm* auf Seite 253.

Erste Schritte 2

Nachdem Sie die VirusScan Enterprise-Software installiert haben, können Sie mit der Konfiguration der Features beginnen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Orientierung auf die Benutzeroberfläche
- Einrichten von Benutzeroberflächenoptionen
- Einrichten von Scan-Vorgängen
- Virusinformationsbibliothek
- Einsenden eines Virenbeispiels
- Einrichten der Remoteverwaltung

Orientierung auf die Benutzeroberfläche

Die VirusScan Enterprise-Software bietet Ihnen ein hohes Maß an Flexibilität, da zur Ausführung der Aktionen verschiedene Methoden verwendet werden können. Obwohl in Bezug auf bestimmte Einzelheiten Unterschiede bestehen, können viele der Aktionen sowohl von der Konsole, der Symbolleiste, einem Menü oder dem Desktop aus ausgeführt werden. Die verschiedenen Methoden werden in den folgenden Abschnitten detailliert beschrieben.

In diesem Abschnitt werden die folgenden Oberflächen erläutert:

- Startmenü
- VirusScan-Konsole
- Kontextmenüs
- Systemablage
- Befehlszeile

Startmenü

Verwendung des Startmenüs:

- Zugriff auf die Konfiguration des Warnungs-Managers, sofern der Warnungs-Manager installiert ist.
- Zugriff auf die **VirusScan-Konsole**.
- Aufrufen der Eigenschaftenseiten für das Scannen bei Zugriff.
- Aufrufen der Eigenschaftenseiten für das Scannen auf Anforderung. Hierbei handelt es sich um einen einmaligen Scan-Vorgang, der auf Anforderung ausgeführt und nicht gespeichert wird.

Klicken Sie auf **Start**, wählen Sie **Programme** | **Network Associates** und dann das gewünschte Feature**.**

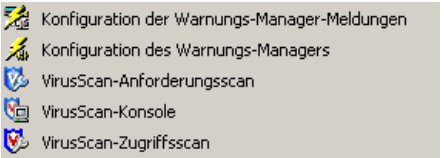


Abbildung 2-1. VirusScan – Startmenü

VirusScan-Konsole

Die **VirusScan-Konsole** ist der zentrale Punkt zur Steuerung der Programmaktivitäten.

Öffnen Sie die **VirusScan-Konsole** mit einer dieser Methoden:

- Klicken Sie auf **Start**, wählen Sie **Programme | Network Associates | VirusScan-Konsole.**
- Klicken Sie mit der rechten Maustaste auf das Symbol *VShield* in der Systemablage und wählen Sie **VirusScan-Konsole**.

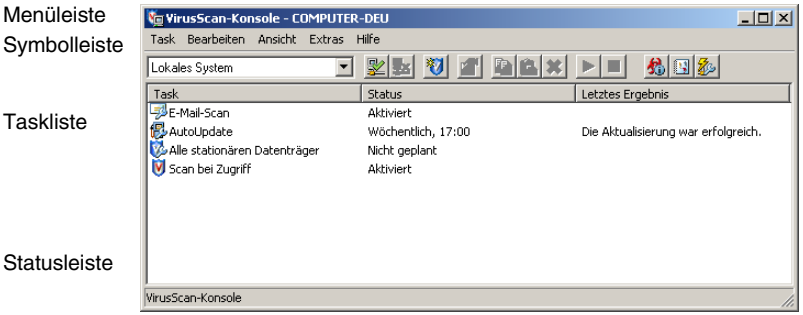


Abbildung 2-2. Die VirusScan-Konsole

In diesem Abschnitt werden die folgenden Themen behandelt:

- Menüleiste
- Symbolleiste
- Taskliste
- Statusleiste

Menüleiste

Die **VirusScan-Konsole** enthält Menüs mit Befehlen, mit deren Hilfe Sie Scan-Tasks erstellen, löschen, konfigurieren, ausführen, abbrechen und kopieren können, um diese an Ihre vordringlichsten Sicherheitsanforderungen anzupassen. Außerdem können Sie von einem VirusScan Enterprise-Remote-Computer aus eine Verbindung aufbauen oder trennen. Auf alle diese Befehle kann über die Menüs zugegriffen werden. Einige Befehle können jedoch auch aufgerufen werden, indem Sie mit der rechten Maustaste in der **VirusScan-Konsole** auf einen Task klicken.

In diesem Abschnitt werden die folgenden Menüs behandelt:

- Menü "Task"
- Menü "Bearbeiten"
- Menü "Ansicht"
- Menü "Extras"
- Menü "Hilfe"

Menü "Task"

Über das Menü **Task** können Sie Tasks erstellen und konfigurieren sowie Statistiken und Aktivitätsprotokolle anzeigen.

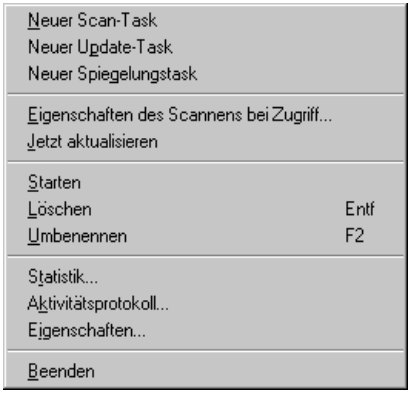


Abbildung 2-3. Menü "Task"

HINWEIS
Die Menüelemente **Start**, **Stopp**, **Deaktivieren**, **Löschen**, **Umbenennen**, **Statistik**, **Aktivitätsprotokoll** und **Eigenschaften** beziehen sich auf den markierten Task.

Menü "Bearbeiten"

Mithilfe der Einträge im Menü **Bearbeiten** können Sie ausgewählte Tasks kopieren und einfügen.

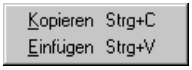


Abbildung 2-4. Menü "Bearbeiten"

Menü "Ansicht"

Über das Menü **Ansicht** können Sie die Konsole aktualisieren oder festlegen, ob die Symbol- und die Statusleiste angezeigt werden sollen.



Abbildung 2-5. Menü "Ansicht"

Menü "Extras"

Im Menü **Extras** können Sie Warnungen konfigurieren, die Ereignisanzeige starten, die Optionen der Benutzeroberfläche angeben, die Sicherheitseinstellungen für die Benutzeroberfläche sperren oder entsperren, einen Computer beim Konfigurieren einer Remote-Konsole verbinden oder trennen, die Repository-Liste importieren oder bearbeiten oder DAT-Dateien auf eine frühere Version zurücksetzen.



Abbildung 2-6. Menü "Extras"

Menü "Hilfe"

Über das Menü **Hilfe** können Sie auf die Online-Hilfethemen, die Virusinformationsbibliothek oder die Website des Technischen Supports zugreifen. Außerdem können Sie ein Virusbeispiel an das Anti-Virus Emergency Response Team (AVERT) senden. Im Dialogfeld **Info** erhalten Sie Informationen zum Produkt, zur DAT-Dateiversion und zum Scan-Modul.

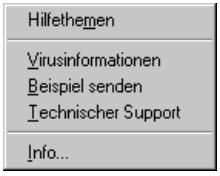


Abbildung 2-7. Menü "Hilfe"

Symbolleiste

Über die Symbolleiste können Sie durch einfaches Klicken auf ein Symbol besonders schnell auf Befehle zugreifen. Mithilfe der Symbole können Sie folgende Aktionen durchführen:

- Eine Verbindung zu einem Computer herstellen
- Eine Verbindung vom Computer trennen
- Einen neuen Task erstellen
- Eigenschaften für das ausgewählte Element anzeigen
- Das ausgewählte Element kopieren
- Das ausgewählte Element einfügen
- Das ausgewählte Element löschen
- Das ausgewählte Element starten
- Das ausgewählte Element stoppen
- Auf die Virusinformationsbibliothek zugreifen
- Die Ereignisanzeige öffnen
- Warnoptionen konfigurieren

Taskliste

In der **VirusScan-Konsole** sind eine Reihe von Tasks aufgelistet, die mit VirusScan Enterprise ausgeführt werden können. Ein *Task* setzt sich aus mehreren Anweisungen zusammen, die in einer bestimmten Konfiguration und zu einer bestimmten Zeit die Ausführung eines Programms oder Scan-Vorgangs bewirken.

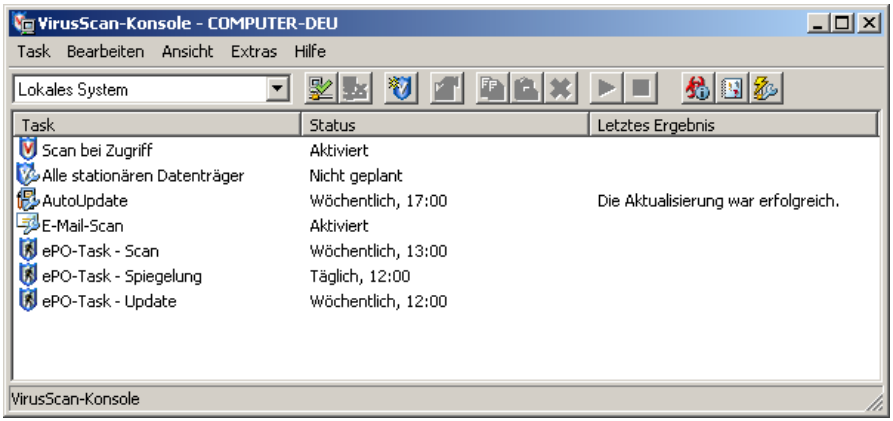


Abbildung 2-8. Taskliste

Um einen Task zu konfigurieren, wählen Sie den Task aus und klicken dann auf  oder doppelklicken auf den Task. Die Eigenschaftenseiten des Tasks werden geöffnet. Im Lieferumfang der VirusScan Enterprise-Software sind die folgenden standardmäßigen Tasks enthalten:

- **Scan bei Zugriff**: Mit diesem Task können Sie automatische Scans bei Zugriff durchführen. Dieser Task kann nicht kopiert werden. Informationen zum Konfigurieren des Scanners bei Zugriff finden Sie unter *Scannen bei Zugriff* auf Seite 45.
- **AutoUpdate**: Mit diesem Task können Sie die aktuellsten Virendefinitionsdateien (DAT) und das Scan-Modul herunterladen. Sie können diesen Standard-Update-Task verwenden oder andere Update-Tasks erstellen, die Ihren Anforderungen entsprechen. Informationen zum Erstellen, Konfigurieren und Planen von Aktualisierungstasks finden Sie unter *Aktualisieren* auf Seite 199.
- **E-Mail-Scan**: Mit diesem Task können Sie E-Mail-Empfangsscans durchführen. Dieser Task kann nicht kopiert werden. Informationen zum Konfigurieren von E-Mail-Tasks bei Empfang oder auf Anforderung finden Sie unter *Scannen von E-Mails* auf Seite 127.

- **Alle stationären Datenträger**: Mit diesem Task können Sie Scans bei Zugriff durchführen. Sie können diesen Scan-Task verwenden oder andere Scan-Tasks erstellen, die Ihren Anforderungen entsprechen. Informationen zum Erstellen, Konfigurieren und Planen von Tasks auf Anforderung finden Sie unter *Scannen auf Anforderung* auf Seite 95.

Andere Tasks, die Sie über die **VirusScan-Konsole** erstellen, werden der Taskliste hinzugefügt. Zum Beispiel:

- **Neuer Spiegelungstask**: Mit diesem Task können Sie eine Spiegelsite zum Herunterladen von Aktualisierungsdateien erstellen. Sie können beliebig viele Spiegelungstasks erstellen. Weitere Informationen über Spiegelungstasks finden Sie unter *Spiegelungstasks* auf Seite 224.

Außerdem haben Sie die Möglichkeit, die erstellten Tasks über ePolicy Orchestrator anzuzeigen.

- **ePO-Task – Task-Name**. Wenn Sie ePolicy Orchestrator 3.0 oder höher zur Verwaltung der VirusScan Enterprise-Software verwenden, können Sie in der **VirusScan-Konsole** ePolicy Orchestrator-Tasks anzeigen. Dies gilt für Anforderungs-, Aktualisierungs- und Spiegelungstasks. Informationen zur Aktivierung der Tasksichtbarkeit für ePolicy Orchestrator finden Sie im *VirusScan Enterprise-Konfigurationshandbuch für die Verwendung mit ePolicy Orchestrator 3.0*.

Statusleiste

In der Statusleiste wird der Status der aktuellen Aktivität angezeigt.

Kontextmenüs

Über die Kontextmenüs erhalten Sie schnell Zugriff auf häufig benötigte Befehle, z. B. zum Erstellen von neuen Tasks, Anzeigen von Task-Statistiken und -Protokollen, Öffnen von Task-Eigenschaftenseiten oder Prüfen von bestimmten Dateien oder Ordnern auf Viren.

- **Kontextmenüs in der Konsole**: Welche Kontextmenüs in der **VirusScan-Konsole** verfügbar sind, hängt davon ab, ob Sie einen Task in der Taskliste ausgewählt haben und um welchen Task es sich dabei handelt. Genauere Informationen finden Sie unter *Kontextmenüs in der Konsole* auf Seite 29.

- **Scannen über rechte Maustaste**: Diese Scan-Funktion im Kontextmenü ermöglicht Ihnen, eine bestimmte Datei oder einen bestimmten Ordner auszuwählen und sofort auf Viren zu prüfen. Genauere Informationen finden Sie unter *Scannen über rechte Maustaste* auf Seite 30.

- **Scannen über das Kontextmenü der Systemablage**: Diese Scan-Funktion im Kontextmenü ermöglicht Ihnen, einen einmaligen, nicht gespeicherten Anforderungsscan-Task zu erstellen. Genauere Informationen finden Sie unter *Scannen oder Aktualisieren über das Kontextmenü der Systemablage* auf Seite 30.

Kontextmenüs in der Konsole

Wenn Sie mit der rechten Maustaste auf einen Eintrag in der Taskliste klicken, stehen Ihnen diese Optionen zur Verfügung:

- **Scan bei Zugriff**: Wenn Sie in der Taskliste mit der rechten Maustaste auf den Scan-Task klicken, der bei Zugriff ausgeführt wird, enthält das Kontextmenü Optionen zum Aktivieren oder Deaktivieren des Tasks, zum Anzeigen der Task-Statistik, zum Anzeigen des Aktivitätsprotokolls und zum Öffnen der Eigenschaftenseiten.
- **Aktualisieren**: Wenn Sie in der Taskliste mit der rechten Maustaste auf einen Aktualisierungs-Task klicken, enthält das Kontextmenü Optionen zum Starten oder Stoppen, Löschen und Umbenennen des Tasks, zum Anzeigen des Aktivitätsprotokolls sowie zum Öffnen der Eigenschaftenseiten.
- **E-Mail-Scan**: Wenn Sie in der Taskliste mit der rechten Maustaste auf einen E-Mail-Scan-Task klicken, der bei Zugriff ausgeführt wird, enthält das Kontextmenü Optionen zum Aktivieren oder Deaktivieren des Tasks, zum Anzeigen der Task-Statistik, zum Anzeigen des Aktivitätsprotokolls und zum Öffnen der Eigenschaftenseiten.
- **Scannen auf Anforderung**: Wenn Sie in der Taskliste mit der rechten Maustaste auf einen Scan-Task klicken, der auf Anforderung ausgeführt wird, enthält das Kontextmenü Optionen zum Starten oder Stoppen, Kopieren oder Einfügen, Löschen und Umbenennen des Tasks, zum Anzeigen der Task-Statistik, zum Anzeigen des Aktivitätsprotokolls und zum Öffnen der Eigenschaftenseiten.

Wenn Sie mit der rechten Maustaste auf einen freien Bereich in der Konsole klicken, *ohne dabei ein Element in der Taskliste auszuwählen*, können Sie diese Aktionen ausführen:

- **Neuer Scan-Task**: Ein neuer Anforderungsscan-Task wird erstellt.
- **Neuer Aktualisierungs-Task**: Ein neuer Aktualisierungs-Task wird erstellt.
- **Neuer Spiegelungstask**: Ein neuer Spiegelungstask wird erstellt.
- **Einfügen**: Ein kopierter Task wird in die Taskliste eingefügt.
- **Benutzeroberflächenoptionen**: Die Eigenschaftenseiten **Benutzeroberflächenoptionen** werden aufgerufen. Informationen zum Festlegen dieser Optionen finden Sie unter *Einrichten von Benutzeroberflächenoptionen* auf Seite 32.

Scannen über rechte Maustaste

Sie können eine ausgewählte Datei oder einen ausgewählten Ordner sofort auf Viren prüfen, indem Sie in Windows-Explorer mit der rechten Maustaste auf die Datei oder den Ordner klicken und die Option **Nach Viren scannen** auswählen. Dies wird auch als *Shell-Erweiterungs-Scan* bezeichnet. Wenn der Anforderungs-Scanner aufgerufen wird, sind alle Scan-Einstellungen, d. h. Archiv-Scan, Heuristik-Scan usw., bereits aktiviert. Dies empfiehlt sich, wenn Sie vermuten, dass ein bestimmter Ordner oder eine bestimmte Datei infiziert sind.

Wenn Dateien oder Ordner infiziert sind, werden sie mit den Details des infizierten Elements unten im Scan-Dialogfeld in einer Listenansicht angezeigt. Sie können für das infizierte Element Maßnahmen ergreifen, indem Sie in der Listenansicht mit der rechten Maustaste auf das Element klicken und die Option zum Säubern, Löschen oder Verschieben wählen.

Beim Scannen über die rechte Maustaste können die Scan-Optionen nicht angepasst werden. Wenn Sie die Scan-Optionen Ihren Bedürfnissen entsprechend anpassen möchten oder einen neuen Anforderungsscan-Task erstellen möchten, siehe *Erstellen von Anforderungstasks* auf Seite 96 für weitere Informationen.

Systemablage

Der Zugriffsscanner wird bei der normalen Installation standardmäßig installiert und aktiviert. Sobald der Scanner aktiviert ist, wird in der Systemablage von Windows das Symbol *Vshield* angezeigt.

Doppelklicken Sie in der Systemablage auf , um **Statistische Daten zum Scannen bei Zugriff** anzuzeigen.

Scannen oder Aktualisieren über das Kontextmenü der Systemablage

Verwenden Sie diese Funktion, um einen einmaligen, nicht gespeicherten Anforderungsscan-Task zu erstellen. Dies ist nützlich, wenn Sie ein Laufwerk, einen Ordner oder eine Datei schnell und zu einem anderen Zeitpunkt als dem regelmäßig eingeplanten Anforderungsscan scannen oder eine direkte Aktualisierung durchführen wollen.

Klicken Sie in der Systemablage mit der rechten Maustaste auf , um das Kontextmenü anzuzeigen.



Abbildung 2-9. Das Menü der Systemablage

Im Menü der Systemablage sind folgende Optionen enthalten:

- **VirusScan-Konsole**: Zeigt die **VirusScan-Konsole** an.
- **Scannen bei Zugriff deaktivieren**: Deaktiviert den Zugriffsscanner.. : Diese Funktion schaltet zwischen **Scannen bei Zugriff deaktivieren** und **Scannen bei Zugriff aktivieren** um.
- **Eigenschaften für Scan bei Zugriff**: Rufen Sie die Eigenschaftenseiten für den Zugriffsscanner auf, um ihn zu konfigurieren.
- **Statistische Daten zum Scannen bei Zugriff**: Mit dieser Option wird die Statistik zum Scannen bei Zugriff angezeigt. Sie können den Zugriffsscanner aktivieren bzw. deaktivieren oder die Eigenschaftenseiten für den Zugriffsscanner aufrufen.
- **Nachrichten vom Scannen bei Zugriff**: Mit dieser Option werden Nachrichten zum Scannen bei Zugriff angezeigt. Sie können Nachrichten entfernen und Dateien säubern, löschen oder verschieben.
- **Scannen auf Anforderung**: Rufen Sie die Eigenschaftenseiten für das Scannen auf Anforderung auf, um den Auftragsscan für einen einmaligen, nicht gespeicherten Auftragsscan zu konfigurieren.
- **Jetzt aktualisieren**: Mit dieser Option wird der Standard-Aktualisierungs-Task sofort aktualisiert.

  HINWEIS
  Die Option **Jetzt aktualisieren** führt nur den Standard-Aktualisierungs-Task aus, der beim Installieren des Produkts erstellt wurde. Sie können den Standard-Task umbenennen und neu konfigurieren. Wenn Sie den Task jedoch löschen, wird die Option **Jetzt aktualisieren** deaktiviert.

- **Info zu VirusScan Enterprise**: Mit dieser Option werden spezifische Informationen über die installierte Software wie die Versionsnummern der Virusdefinitionsdatei (DAT) und des Scan-Moduls sowie Lizenzinformationen zum Produkt angezeigt.

Befehlszeile

Verwenden Sie das Feature Befehlszeile, um Aktivitäten über das Befehlseingabefenster auszuführen. Weitere Informationen finden Sie unter *Befehlszeilen-Scannerprogramm* auf Seite 253.

Einrichten von Benutzeroberflächenoptionen

Verwenden Sie diese Optionen, um Anzeige- und Kennwortoptionen bei der Programminstallation mithilfe von McAfee Installation Designer oder danach im Menü **Extras** in der **VirusScan-Konsole** festzulegen.

Im Folgenden wird beschrieben, wie die Anzeige- und Kennwortoptionen über die Konsole eingerichtet werden. In diesem Abschnitt werden die folgenden Themen behandelt:

- Anzeigeoptionen
- Kennwortoptionen
- Entsperren und Sperren der BenutzeroberflächeEntsperren und Sperren der Benutzeroberfläche

Anzeigeoptionen

Im Dialogfeld **Anzeigeoptionen** können Sie festlegen, auf welche Optionen der Systemablage Benutzer zugreifen können, und Sie können die Aktualisierungszeit für die lokale Konsole einrichten.

So werden die Anzeigeoptionen über die Konsole eingerichtet:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie **Extras** | **Benutzeroberflächenoptionen** | **Anzeigeoptionen**.

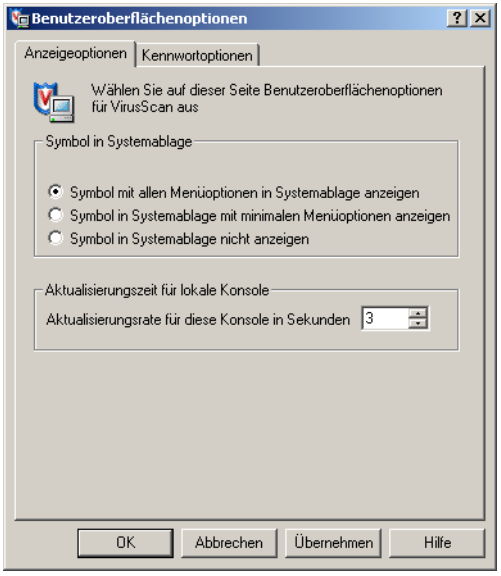


Abbildung 2-10. Anzeigeoptionen

3. Legen Sie fest, welche Systemablageoptionen den Benutzern angezeigt werden sollen. Wählen Sie unter **Symbol in Systemablage** eine der folgenden Optionen:
   - **Symbol mit allen Menüoptionen in Systemablage anzeigen**: *Diese Option ist standardmäßig ausgewählt.* Den Benutzern sollen in der Systemablage alle Menüoptionen angezeigt werden.
   - **Symbol in Systemablage mit minimalen Menüoptionen anzeigen**: In den Kontextmenüs sind nur die Optionen **Info** und **Statistische Daten zum Scannen bei Zugriff** verfügbar. Alle anderen Optionen des Kontextmenüs sind ausgeblendet.
   - **Symbol in Systemablage nicht anzeigen**: Die Benutzer können nicht auf das Symbol in der Systemablage zugreifen.

4 Wählen Sie unter **Aktualisierungszeit für lokale Konsole** die Abstände (in Sekunden) aus, in denen in die Konsole aktualisiert werden soll.

5 Klicken Sie auf **Anwenden** und anschließend auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld zu schließen.

Kennwortoptionen

Im Dialogfeld **Kennwortoptionen** können Sie ein Sicherheitskennwort für das gesamte System oder nur für ausgewählte Registerkarten und Steuerelemente festlegen. Bei allen ausgewählten Registerkarten und Steuerelementen wird dasselbe Kennwort verwendet.

Der Kennwortschutz hat folgende Auswirkungen auf die Benutzer:

Nicht-Administratoren: *Benutzer ohne Windows NT-Administratorrechte*. Benutzer ohne Administratorrechte führen alle **VirusScan Enterprise**-Anwendungen immer im schreibgeschützten Modus aus. Sie können einige Konfigurationsparameter anzeigen, gespeicherte Scan-Tasks ausführen und sofortige Scans und Aktualisierungen durchführen. Sie können jedoch keine Konfigurationsparameter ändern oder gespeicherte Scan- oder Aktualisierungs-Tasks erstellen, löschen oder bearbeiten.

Administratoren: *Benutzer mit Windows NT-Administratorrechten*. Wenn *kein* Kennwort festgelegt ist, führen Administratoren alle VirusScan Enterprise-Anwendungen im Lese-/Schreib-Modus aus. Sie können alle Konfigurationsparameter anzeigen und ändern, Tasks ausführen sowie gespeicherte Scan- und Aktualisierungs-Tasks erstellen, löschen oder bearbeiten. Wenn ein Kennwort *festgelegt*, aber nicht eingegeben wurde, werden den Administratoren die geschützten Registerkarten und Steuerelemente im schreibgeschützten Modus angezeigt. Administratoren können die Benutzeroberfläche über die Konsole sperren und entsperren. Weitere Informationen finden Sie unter *Entsperren und Sperren der Benutzeroberfläche* auf Seite 37.

HINWEIS
Ein geschlossenes rotes Vorhängeschloss weist darauf hin, dass für das Element ein Kennwort benötigt wird. Wenn ein offenes grünes Vorhängeschloss angezeigt wird, ist der Lese- und Schreibzugriff auf das Element gewährt.

So werden die Kennwortoptionen über die Konsole eingerichtet:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Wählen Sie **Extras** | **Benutzeroberflächenoptionen** | **Kennwortoptionen**.

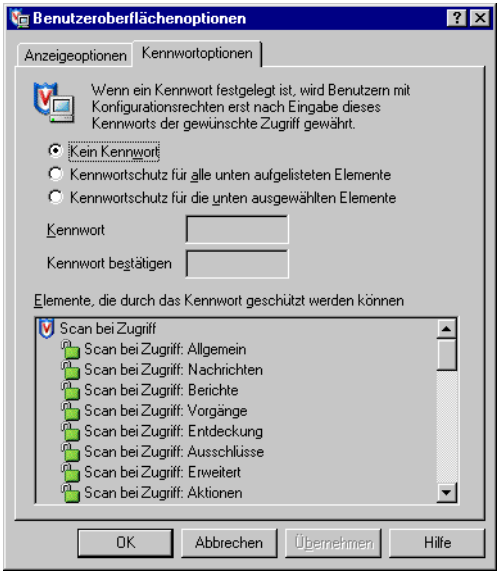


Abbildung 2-11. Kennwortoptionen

3 Wählen Sie eine der folgenden Optionen aus:

- **Kein Kennwort**: *Diese Option ist standardmäßig ausgewählt.*
- **Kennwortschutz für alle unten aufgelisteten Elemente**: Die Benutzer müssen erst das angegebene Kennwort eingeben, bevor sie in der Software auf gesperrte Registerkarten oder Steuerelemente zugreifen können.
  - Wählen Sie **Kennwortschutz für alle unten aufgelisteten Elemente**.
  - Geben Sie das Kennwort ein und bestätigen Sie es.

- **Kennwortschutz für die unten ausgewählten Elemente**. Die Benutzer müssen erst das angegebene Kennwort eingeben, bevor sie auf die hier von Ihnen gesperrten Elemente zugreifen können. Alle nicht gesperrten Elemente erfordern kein Kennwort.
  - Wählen Sie **Kennwortschutz für die unten ausgewählten Elemente**.
  - Geben Sie das Kennwort ein und bestätigen Sie es.
  - Wählen Sie alle Elemente aus, für die dieses Kennwort gelten soll.

4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
5. Klicken Sie auf **OK**.

WARNUNG

Wenn das Kennwortelement **Konsole und Verschiedenes** gesperrt ist, ist die Ausführung der folgenden Vorgänge nicht möglich:

- Aktivieren bzw. Deaktivieren des Scannens bei Zugriff – Die Menüelemente zum Aktivieren bzw. Deaktivieren des Scannens bei Zugriff und die entsprechenden Symbole in der Symbolleiste sind deaktiviert. Außerdem ist die Schaltfläche **Deaktivieren** im Dialogfeld **Statistische VirusScan-Daten zum Scannen bei Zugriff** deaktiviert.
- Aktivieren bzw. Deaktivieren des E-Mail-Scannens – Die Menüelemente zum Aktivieren bzw. Deaktivieren des E-Mail-Scannens und die entsprechenden Symbole in der Symbolleiste sind deaktiviert. Außerdem ist die Schaltfläche **Deaktivieren** im Dialogfeld **Statistik für das Scannen von E-Mails mit VirusScan beim Empfang** deaktiviert.
- Erstellen eines neuen Anforderungsscan-Tasks, Aktualisierungs-Tasks oder Spiegelungstasks – Die Menüelemente zum Erstellen neuer Tasks und die entsprechenden Symbole in der Symbolleiste sind deaktiviert. Zusätzlich sind für Aufforderungsscan-Tasks die Schaltflächen **Speichern unter** und **Als Standard speichern** im Dialogfeld **VirusScan-Eigenschaften des Scans auf Anforderung** deaktiviert.
- Löschen von Tasks – Das Menüelement zum Löschen von Tasks und das entsprechende Symbol in der Symbolleiste sind deaktiviert.
- Umbenennen von Tasks – Das Menüelement zum Umbenennen von Tasks und das entsprechende Symbol in der Symbolleiste sind deaktiviert.
- Kopieren bzw. Einfügen von Tasks – Die Menüelemente zum Kopieren und Einfügen von Tasks und die entsprechenden Symbole in der Symbolleiste sind deaktiviert
- Zurückführen der DAT-Dateien – Das Menüelement zum Zurückführen der DAT-Dateien ist deaktiviert.

Entsperren und Sperren der Benutzeroberfläche

Administratoren können geschützte Registerkarten und Steuerelemente über die Konsole entsperren und sperren.

> **HINWEIS**
> Wenn ein Element durch ein Kennwort geschützt ist, ist auch automatisch das Dialogfeld **Benutzeroberflächenoptionen** geschützt. Wenn für ein Element ein Kennwortschutz eingestellt wurde, wird die Benutzeroberfläche automatisch nach der Abmeldung des Benutzers erneut gesperrt.

So entsperren Sie die Benutzeroberfläche:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie **Extras** | **Benutzeroberfläche entsperren**.

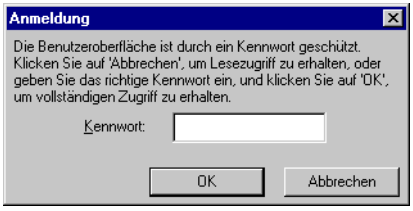

Anmeldung
Die Benutzeroberfläche ist durch ein Kennwort geschützt. Klicken Sie auf 'Abbrechen', um Lesezugriff zu erhalten, oder geben Sie das richtige Kennwort ein, und klicken Sie auf 'OK', um vollständigen Zugriff zu erhalten.
Kennwort:
OK
Abbrechen

Abbildung 2-12. Sicherheitskennwort

3. Geben Sie das Kennwort ein.
4. Klicken Sie auf **OK**.

So sperren Sie die Benutzeroberfläche:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie **Extras auswählen** | **Benutzeroberfläche sperren**.

Einrichten von Scan-Vorgängen

Die VirusScan Enterprise-Software bietet für verschiedene Ansprüche unterschiedliche Scantypen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Scannen bei Zugriff im Vergleich zum Scannen auf Anforderung
- Automatisches Scannen
- Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten

Scannen bei Zugriff im Vergleich zum Scannen auf Anforderung

Die VirusScan Enterprise-Software enthält zwei Arten von Scan-Aktivitäten. Sie können folgende Scan-Aktivitäten ausführen:

- Automatisches Scannen
- Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten

Scannen bei Zugriff: Die automatische Virenprüfung wird als Scannen bei Zugriff bezeichnet. Sie müssen über Administratorrechte und gegebenenfalls über das entsprechende Kennwort verfügen, um das Scannen bei Zugriff konfigurieren zu können. Weitere Informationen finden Sie unter *Automatisches Scannen* auf Seite 39.

Scannen auf Anforderung: Das Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten wird als Scannen auf Anforderung bezeichnet. Um einen Scan-Task auf Anforderung zu planen, benötigen Sie Administratorrechte und gegebenenfalls das entsprechende Kennwort. Der Scan-Task kann jedoch von allen Benutzern ausgeführt werden. Weitere Informationen finden Sie unter *Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten* auf Seite 40.

Da der Zugriffsscanner Ihren Computer mit einem dauerhaften, im Hintergrund laufenden Schutz ausstattet, mag die Ausführung von Scan-Tasks auf Anforderung überflüssig erscheinen. Optimale Sicherheitsmaßnahmen für den Virenschutz umfassen jedoch vollständige und regelmäßige System-Scans. Das hat folgende Gründe:

- **Bei Scan-Vorgängen auf Zugriff werden die Dateien beim des Zugriff oder bei der Verwendung geprüft.** Der Zugriffsscanner sucht nach Viren, während die Dateien verwendet werden. Wenn es auf Ihrem System infizierte Dateien gibt, die jedoch selten benötigt werden, wird der Virus vom Zugriffsscanner erst bei Verwendung der Datei erkannt. Im Rahmen der auf Anforderung ausgeführten Scan-Vorgänge können Viren in auf der Festplatte abgelegten Dateien auch dann erkannt werden, wenn sie noch nie verwendet wurden. Scan-Vorgänge auf Anforderung erkennen Viren vor der Ausführung einer Datei.

- **Viren treten unerwartet auf.** Wenn Sie versehentlich eine Diskette im Laufwerk lassen und den Computer starten, kann es passieren, dass sich ein Virus vor dem Start des Zugriffsscan-Dienstes in den Speicher lädt. Diese Gefahr besteht vor allem dann, wenn der Dienst nicht für das Scannen von Diskettenlaufwerken konfiguriert wurde. Sobald ein gefährlicher Virus in den Speicher gelangt ist, können fast alle Programme von ihm infiziert werden.
- **Das Scannen bei Zugriff kostet Zeit und Ressourcen.** Durch das Scannen nach Viren beim Ausführen, Kopieren oder Speichern von Dateien kann sich das Laden von Anwendungen und anderen Tasks verlangsamen. Das kann je nach Situation genau die Zeit sein, die Ihnen dann bei wichtigen Aufgaben fehlt. Obgleich die Systemleistung nur unwesentlich beeinträchtigt wird, sind Sie möglicherweise versucht, den Zugriffsscanner zu deaktivieren, um jedes Bit des Arbeitsspeichers für speicherintensive Tasks zu nutzen. In diesem Fall kann der Virenschutz des Systems durch Scan-Vorgänge gewährleistet werden, die regelmäßig während des Leerlaufs eines Systems durchgeführt werden. Die Systemleistung wird dabei nicht beeinträchtigt.
- **In Bezug auf Sicherheit gilt: Je redundanter desto besser.** In der vernetzten, Internet-fokussierten Computerwelt unserer Zeit reichen manchmal schon Bruchteile von Sekunden aus, um Viren von Quellen herunterzuladen, die noch nicht einmal bewusst besucht wurden. Wenn das Hintergrund-Scannen aufgrund eines Software-Konflikts genau in diesem Moment deaktiviert war oder gar nicht erst konfiguriert wurde, können Sie das System dabei schon mit einem Virus infiziert haben. Regelmäßige Scan-Vorgänge können auftretende Viren abfangen, bevor diese sich ausbreiten oder Schaden anrichten.

Automatisches Scannen

Durch das Scannen bei Zugriff ist gewährleistet, dass Viren auf der Grundlage der Benutzeraktivitäten fortlaufend und in Echtzeit erkannt und entsprechend behandelt werden. Im Lieferumfang des Virenschutzprogramms VirusScan Enterprise ist ein einzelner Scan-Task bei Zugriff enthalten, der das System immer dann auf Infektionen prüft, wenn ein Netzwerkbenutzer eine Datei auf den Computer schreibt oder von diesem liest. Der Scanner versucht, die erkannten Infektionen zu säubern, und schreibt seine Aktivitäten in eine Protokolldatei. Die Einstellungen für diesen Task können geändert werden, um Folgendes festzulegen:

- Die Dateien oder Dateiformate, die gescannt werden sollen.
- Die Bedingungen für den Start eines Scan-Vorgangs.
- Die vom Scanner bei Erkennung einer Infektion auszuführende Aktion.
- Den Inhalt (falls vorhanden) des Aktivitätsprotokolls des Scanners.
- Die vom Scannen bei Zugriff auszuschließenden Dateien.

Weitere Einzelheiten zum Scannen bei Zugriff finden Sie unter *Scannen bei Zugriff* auf Seite 45.

Scannen in regelmäßigen Abständen, bei Auswahl oder zu festgelegten Zeiten

Bei Anforderungsscan-Tasks werden zwei Typen unterschieden:

- Einmalige Anforderungsscan-Tasks, die nicht gespeichert werden.
- Gespeicherte Anforderungsscan-Tasks.

Einmalige, nicht gespeicherte Anforderungsscan-Tasks können zwar konfiguriert und geplant werden, sie werden jedoch nur für eine spätere Verwendung gespeichert, wenn Sie dies explizit festlegen.

Gespeicherte Anforderungsscan-Tasks können im Voraus geplant und dann, entweder regelmäßig oder wenn Ihrer Meinung nach die Notwendigkeit besteht ausgeführt werden. In Bezug auf die Anzahl der für bestimmte Speicherpfade im Netzwerk erstellten Scan-Tasks ist keine Obergrenze festgelegt. Die Tasks können sehr spezifisch, für ein bestimmtes Laufwerk, ein Verzeichnis oder eine Datei, bzw. auch umfassender, für mehrere Laufwerke, Verzeichnisse oder Dateien, definiert werden. Nach der Erstellung sind die gespeicherten Scan-Tasks so lange verfügbar, bis sie wieder aus der **VirusScan-Konsole** gelöscht werden. Sie können nach Bedarf bearbeitet werden.

Umfassende Erläuterungen zum Einrichten von Anforderungsscan-Aktivitäten finden Sie unter *Scannen auf Anforderung* auf Seite 95.

Virusinformationsbibliothek

In der AVERT-Virusinformationsbibliothek von McAfee sind genaue Informationen über den Ursprungsort von Viren, die Art und Weise, in der sie das System infizieren, und Vorgehensweisen zum Entfernen der Viren gespeichert.

Neben echten Viren enthält die Virusinformationsbibliothek auch nützliche Informationen zu Scherzviren. Scherzviren sind E-Mail-Warnungen über Anlagendateien, die angeblich Datenträger zerstören. Zwei besonders bekannte Scherzviren sind *A Virtual Card For You* und *SULFNBK*, aber natürlich gibt es unzählige weitere Viren dieser Art. Wenn Sie das nächstemal eine gut gemeinte Virenwarnung erhalten, sollten Sie, bevor Sie die Warnung an Ihren gesamten Freundeskreis weiterleiten, die Authentizität des Virus auf unserer Scherzvirenseite prüfen.

So greifen Sie auf die Virusinformationsbibliothek zu:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

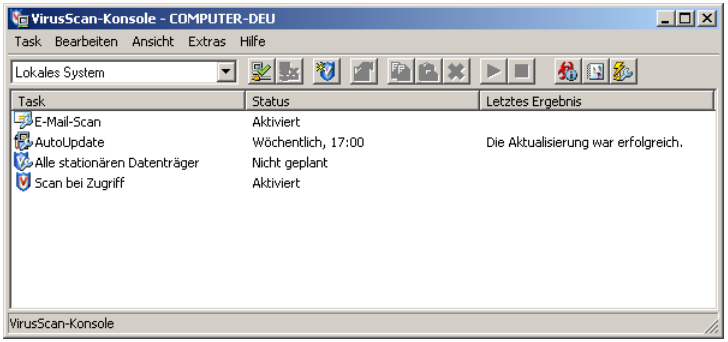


Abbildung 2-13. VirusScan-Konsole

2 Wählen Sie im Menü **Hilfe** die Option **Virusinformationen**.

Einsenden eines Virenbeispiels

Wenn Sie eine verdächtige Datei haben, von der Sie annehmen, dass sie einen Virus enthält, oder das Verhalten des Systems auf eine Infektion hinweist, empfiehlt Ihnen McAfee Security ein Beispiel zur Analyse an das Antiviren-Forschungsteam zu senden. Die Einsendung eines Virus zieht nicht nur eine Analyse, sondern ggf. auch eine Virenbeseitigung nach sich.

So senden Sie ein Virusbeispiel an AVERT:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Wählen Sie aus dem Menü **Hilfe** die Option **Beispiel senden**.

3 Befolgen Sie die Anweisungen auf der Website.

Einrichten der Remoteverwaltung

Sie können Vorgänge ausführen, z. B. das Scannen ändern oder planen, Tasks aktualisieren oder den Zugriffsscanner auf einem Remote-Computer aktivieren oder deaktivieren. Dazu benötigen Sie Administratorrechte, und der Remote-Registrierungsdienst muss ausgeführt werden.

> **HINWEIS**
> Wenn Sie zum Herstellen einer Verbindung mit dem Remote-Computer nicht über die erforderlichen Administratorrechte verfügen, wird die Fehlermeldung *Zugriff aufgrund unzureichender Benutzerrechte verweigert* angezeigt.

Beim Starten der **VirusScan-Konsole** wird in der Titelleiste der Konsole und im Menü links in der Symbolleiste der Konsole der Name des Computers angezeigt, mit dem Sie verbunden sind. In der Titelleiste wird der Name Ihres lokalen Rechners angezeigt, wenn keine Verbindung zu einem anderen Netzwerkcomputer besteht.

Zur Verwaltung eines Remote-Computers, auf dem das Programm VirusScan Enterprise installiert ist, gehen Sie folgendermaßen vor:

1 Wählen Sie aus dem Menü **Extras** die Option **Remote-Verbindung** oder klicken Sie in der Symbolleiste auf  .

Das Dialogfeld **Mit Remote-Computer verbinden** wird angezeigt.

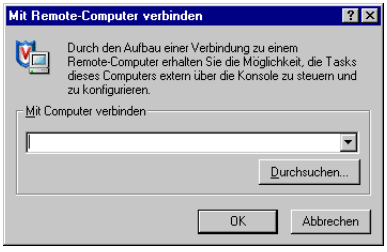

Mit Remote-Computer verbinden
Durch den Aufbau einer Verbindung zu einem Remote-Computer erhalten Sie die Möglichkeit, die Tasks dieses Computers extern über die Konsole zu steuern und zu konfigurieren.
Mit Computer verbinden
Durchsuchen...
OK
Abbrechen

Abbildung 2-14. Verbindung zum Remote-Computer herstellen

2 Klicken Sie auf  , um in der Liste **Mit Computer verbinden** einen Computer auszuwählen, oder geben Sie den Namen des zu verwaltenden Computers in das Textfeld ein. Sie können auch auf die Schaltfläche **Durchsuchen** klicken, um den Computer im Netzwerk zu suchen.

HINWEIS
Wenn beim Konfigurieren des Pfadnamens der Datei oder des Ordners für einen Remote-Task Umgebungsvariablen verwendet werden, müssen Sie sicherstellen, dass die Umgebungsvariable auf dem Remote-Computer vorhanden ist. Die **VirusScan-Konsole** kann Umgebungsvariablen auf dem Remote-Computer nicht überprüfen.

3 Klicken Sie auf **OK**, um eine Verbindung zum Zielcomputer herzustellen.

HINWEIS
Beim Herstellen einer Verbindung mit dem Remote-Computer wird der Name des Computers in der Titelleiste angezeigt und die Taskliste enthält nun die Tasks des Remote-Computers. Sie können Tasks für den Remote-Computer hinzufügen, löschen oder neu konfigurieren.

Die **Konsole** liest die Registrierung des Remote-Computers und zeigt die Tasks des Remote-Computers an. Sobald die Tasks in der Konsole angezeigt werden, können Sie sie auf einem lokalen Computer ausführen.

Um die Verbindung zu einem Computer zu *trennen*, klicken Sie in der Symbolleiste der Konsole auf  oder wählen Sie aus dem Menü **Extras** die Option **Computer trennen**. Wenn Sie die Verbindung zum Remote-Computer trennen, wird die Konsole aktualisiert und die Tasks des lokalen Computers werden angezeigt.

Scannen bei Zugriff 3

Das Antiviren-Programm VirusScan Enterprise verwendet den Zugriffsscanner, um auf der Basis der von Ihnen konfigurierten Einstellungen eine kontinuierliche Virenerkennung und entsprechende Reaktionen in Echtzeit auf Ihrem Computer zu ermöglichen. Sie können vorgangsbasiertes Scannen konfigurieren, bei dem die Scan-Richtlinien mit Anwendungen wie dem Internet Explorer verknüpft werden können.

Wenn eine Infektion erkannt wird, zeichnet der Zugriffsscanner eine Meldung mit Einzelheiten zur infizierten Datei auf und ermöglicht Ihnen, schnell auf die Meldung zuzugreifen und Sofortmaßnahmen an der infizierten Datei durchzuführen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Konfigurieren des Zugriffsscanners
- Anzeigen von Scan-Ergebnissen
- Reaktionen auf die Erkennung von Viren

Konfigurieren des Zugriffsscanners

Für einen optimalen Einsatz des Programms auf Ihrem Computer oder in der Netzwerkumgebung müssen Sie das Programm konfigurieren, um anzugeben, welche Scanvorgänge durchgeführt werden sollen, wie beim Entdecken eines Virus reagiert werden soll und wie Sie in einem solchen Fall benachrichtigt werden möchten.

In der Standardkonfiguration des Zugriffsscanners sind die meisten Reaktionsoptionen aktiviert. Der Scanner ist standardmäßig darauf eingestellt, einen gefundenen Virus zu entfernen. Wenn der Virus nicht entfernt werden kann, wird der Virus in einem Quarantäneordner abgelegt. Der Vorfall wird außerdem in der Protokolldatei erfasst.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Eigenschaften des Scannens bei Zugriff
- Allgemeine Einstellungen
- Vorgangseinstellungen
- Hinzufügen von Dateityperweiterungen
- Hinzufügen benutzerdefinierter Dateityperweiterungen
- Ausschließen von Dateien, Ordnern und Laufwerken

Eigenschaften des Scannens bei Zugriff

So konfigurieren Sie den Zugriffsscanner:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

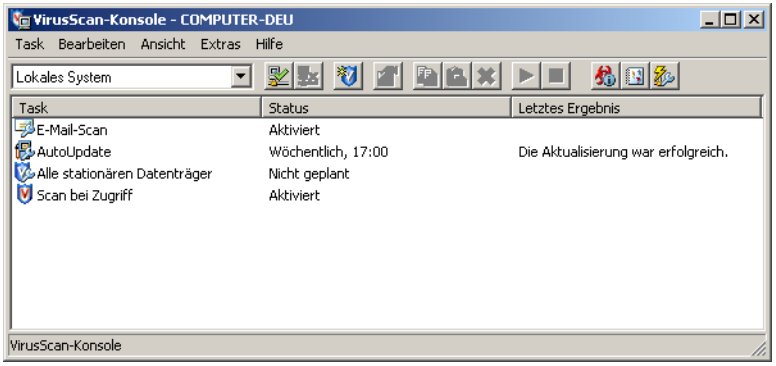


Abbildung 3-1. VirusScan-Konsole

2 Öffnen Sie **Eigenschaften des Scannens bei Zugriff** mithilfe einer der folgenden Methoden:

- Wählen Sie aus dem Menü **Task** der Konsole die Option **Eigenschaften des Scannens bei Zugriff**.
- Klicken Sie in der Konsole mit der rechten Maustaste auf **Scan bei Zugriff** und wählen Sie dann die Option **Eigenschaften**.
- Doppelklicken Sie in der Konsole auf **Scan bei Zugriff**.
- Markieren Sie in der Konsole **Scan bei Zugriff** und klicken Sie anschließend in der Symbolleiste der Konsole auf .
- Klicken Sie in der Systemablage mit der rechten Maustaste auf und wählen Sie anschließend die Option **Eigenschaften für Scan bei Zugriff**.
- Klicken Sie auf **Start** und wählen Sie anschließend **Programme** | **Network Associates** | **VirusScan-Zugriffsscan**.

Das Dialogfeld **Eigenschaften des Scannens bei Zugriff** wird angezeigt.

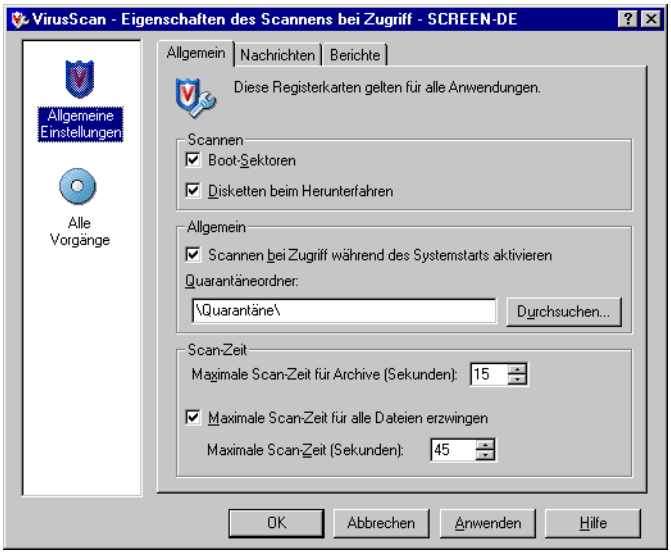


Abbildung 3-2. Eigenschaften des Scannens bei Zugriff – Standardansicht

Im Dialogfeld **Eigenschaften des Scannens bei Zugriff** können Sie allgemeine Einstellungen und drei Vorgangstypen konfigurieren. Mithilfe der Symbole im linken Bereich des Dialogfelds können Sie auf die konfigurierbaren Optionen für folgende Funktionen zugreifen:

Wenn das Dialogfeld **Eigenschaften des Scannens bei Zugriff** erstmals geöffnet wird, bietet die Standardansicht Zugriff auf die Eigenschaften für **Allgemeine Einstellungen** und **Alle Vorgänge**.

- **Allgemeine Einstellungen**: Legen Sie allgemeine Erkennungs-, Benachrichtigungs- und Berichtseigenschaften für *alle* Vorgänge fest. Informationen zum Festlegen dieser Eigenschaften finden Sie unter *Allgemeine Einstellungen* auf Seite 49.
- **Alle Vorgänge** Stellen Sie ein, ob Sie für alle Vorgänge dieselben Vorgangs-, Erkennungs-, erweiterten und Aktionseigenschaften oder für Standardvorgänge und Vorgänge mit geringem und/oder hohem Risiko jeweils unterschiedliche Eigenschaften festlegen möchten. Informationen zum Festlegen dieser Eigenschaften finden Sie unter *Vorgangseinstellungen* auf Seite 56.

Allgemeine Einstellungen

Die Eigenschaften, die Sie unter **Allgemeine Einstellungen** angeben, werden für Standardvorgänge und Vorgänge mit geringem und hohem Risiko angewendet.

Diese Eigenschaften können konfiguriert werden:

- Allgemeine Eigenschaften
- Benachrichtigungseigenschaften
- Berichtseigenschaften

Allgemeine Eigenschaften

Klicken Sie auf die Registerkarte **Allgemein**, um die Basiseigenschaften für das Scannen bei Zugriff zu konfigurieren.

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Allgemeine Einstellungen**.
2. Wählen Sie die Registerkarte **Allgemein** aus.

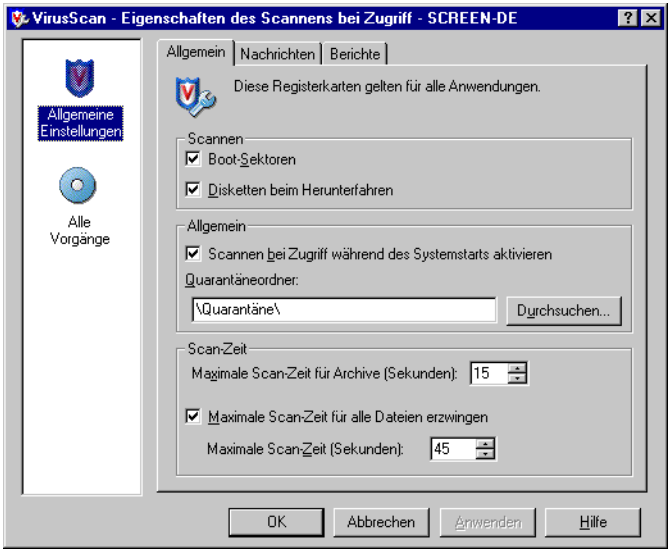


Abbildung 3-3. Allgemeine Einstellungen – Registerkarte "Allgemein"

3 Wählen Sie unter **Scan-Optionen** aus, welche Teile des Computers vom Scanner überprüft werden sollen. Wählen Sie eine der folgenden Optionen aus:

- **Boot-Sektoren**: *Diese Option ist standardmäßig ausgewählt.* Der Boot-Sektor der Festplatte wird in die Scan-Aktivitäten einbezogen. Beim Mounten einer Festplatte berücksichtigt der Scanner den Boot-Sektor der Festplatte. In einigen Fällen kann es angebracht sein, die Analyse des Boot-Sektors zu deaktivieren, z. B. wenn eine Festplatte einen speziellen oder anormalen Boot-Sektor besitzt, der keinem Viren-Scan unterzogen werden kann.
- **Disketten beim Herunterfahren**: *Diese Option ist standardmäßig ausgewählt.* Der Boot-Sektor von Disketten, die sich beim Herunterfahren des Computers noch im Diskettenlaufwerk befinden, wird gescannt. Wenn die Diskette infiziert ist, wird der Computer nicht heruntergefahren, bevor die Diskette entnommen wurde.

4 Wählen Sie unter **Allgemein** eine dieser Optionen:

- **Scannen bei Zugriff während des Systemstarts aktivieren**: *Diese Option ist standardmäßig ausgewählt.* Der Dienst zum Scannen bei Zugriff wird gestartet, wenn Sie Ihren Computer starten.
- **Quarantäneordner**: Übernehmen Sie das Standardverzeichnis und den Namen des Quarantäneordners, geben Sie einen Pfad zu einem anderen Verzeichnis für den Quarantäneordner ein oder klicken Sie auf **Durchsuchen**, um einen geeigneten Ordner auf der lokalen Festplatte auszuwählen.

  Der Standardspeicherort und der Name des Quarantäneordners lautet:

  ```
  <Laufwerk>:\quarantine
  ```

  HINWEIS
  Der *Quarantäneordner* darf nicht auf einer Diskette oder einem CD-Laufwerk, sondern muss auf der Festplatte gespeichert werden.

5 Legen Sie unter **Scan-Zeit** für alle Dateien die maximale Scan-Zeit für Archive in Sekunden fest. Beansprucht der Scan-Vorgang für eine Datei mehr als die angegebene Scan-Zeit, wird der Scan gestoppt und eine entsprechende Meldung protokolliert. Wenn der Scan-Vorgang nicht problemlos gestoppt werden kann, wird er beendet und neu gestartet, wobei eine entsprechend andere Meldung protokolliert wird. Wählen Sie eine der folgenden Optionen aus:

- **Maximale Scan-Zeit für Archive (Sekunden):** *Die Standardeinstellung beträgt 15 Sekunden.* Übernehmen Sie die Standardeinstellung oder wählen Sie aus, wie viele Sekunden der Scanner maximal für das Scannen einer Archiv-Datei verwenden soll. Die für das Scannen von Archiv-Dateien ausgewählte Zeitspanne muss geringer sein als die für das Scannen aller Dateien ausgewählte Zeitspanne.

- **Maximale Scan-Zeit für alle Dateien erzwingen:** *Diese Option ist standardmäßig ausgewählt.* Definiert für alle Dateien eine maximale Scan-Zeit, die dann erzwungen wird.
- **Maximale Scan-Zeit (Sekunden):** *Die Standardeinstellung beträgt 45 Sekunden.* Übernehmen Sie die Standardeinstellung oder wählen Sie aus, wie viele Sekunden der Scanner maximal für das Scannen einer Datei verwenden soll.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Benachrichtigungseigenschaften

Klicken Sie auf die Registerkarte **Nachrichten**, um die allgemeinen Nachrichteneigenschaften der Benutzer für das Scannen bei Zugriff zu konfigurieren.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Allgemeine Einstellungen**.

2 Wählen Sie die Registerkarte **Nachrichten**.



Abbildung 3-4. Allgemeine Einstellungen – Registerkarte "Nachrichten"

3 Wählen Sie unter **Nachrichten für lokale Benutzer** die gewünschten Nachrichtenoptionen aus. Einige dieser Optionen gelten für alle Benutzer, einige gelten nur für Benutzer ohne Administratorenrechte.

Diese Optionen gelten für alle Benutzer:

- **Bei Entdeckung eines Virus Nachrichtendialogfeld anzeigen**: *Diese Option ist standardmäßig ausgewählt.* Zeigt das Dialogfeld **Nachrichten vom Scannen bei Zugriff** an, wenn ein Virus erkannt wird. Weitere Informationen zum Dialogfeld **Nachrichten vom Scannen bei Zugriff** finden Sie unter *Reaktionen auf die Erkennung von Viren* auf Seite 89.

- **Anzuzeigender Text der Nachricht**: Wenn Sie die Option **Bei Entdeckung eines Virus Nachrichtendialogfeld anzeigen** ausgewählt haben, können Sie die Standardnachricht übernehmen oder in das Textfeld eine benutzerdefinierte Nachricht eingeben, die bei der Erkennung von Viren angezeigt wird. *Die Standardnachricht lautet "VirusScan-Warnung!".*

Die nachstehenden Optionen gelten für Aktionen, die Benutzer ohne Administratorrechte an Nachrichten vornehmen können, die im Dialogfeld **Nachrichten vom Scannen bei Zugriff** angezeigt werden. Wählen Sie eine beliebige Kombination dieser Optionen:

- **Nachrichten aus der Liste entfernen**: *Diese Option ist standardmäßig ausgewählt.* Ermöglicht Benutzern ohne Administratorrechte, Nachrichten aus der Liste zu entfernen.

- **Infizierte Dateien säubern**: *Diese Option ist standardmäßig ausgewählt.* Ermöglicht Benutzern ohne Administratorrechte, infizierte Dateien zu bereinigen, auf die von den Nachrichten in der Liste verwiesen wird.

- **Infizierte Dateien löschen**: Ermöglicht Benutzern ohne Administratorrechte, infizierte Dateien zu löschen, auf die von den Nachrichten in der Liste verwiesen wird.

- **Infizierte Dateien in den Quarantäneordner verschieben**: *Diese Option ist standardmäßig ausgewählt.* Ermöglicht Benutzern ohne Administratorrechte, infizierte Dateien in den Quarantäneordner zu verschieben, auf die von den Nachrichten in der Liste verwiesen wird.

4 Wählen Sie unter **Antwort an Netzwerkbenutzer** eine dieser Optionen:

- **Nachricht an Benutzer senden:** Bei Entdeckung eines Virus wird eine Nachricht an den Netzwerkbenutzer gesendet. Dabei kann es sich beispielsweise um eine Warnung an einen Netzwerkbenutzer handeln, der einen Remote-Computer verwendet und über eine Netzwerkfreigabe auf das geschützte Dateisystem zugreift.

  Wenn Sie diese Option auswählen, können Sie die Standardnachricht übernehmen oder eine benutzerdefinierte Nachricht in das dafür vorgesehene Textfeld eingeben. *Die Standardnachricht lautet "Viruswarnung!".*

  WARNUNG
  Der Windows Messenger-Dienst muss ausgeführt werden, um diese Nachricht empfangen zu können.

- **Remote-Benutzer trennen und Zugriff auf freigegebenes Netzwerkverzeichnis verweigern**: Alle Benutzer, die infizierte Dateien in freigegebenen Ordnern auf Ihrem Computer lesen bzw. schreiben, werden automatisch getrennt. Der Scanner erstellt anschließend die Berechtigungen neu, um den Benutzer auszuschließen, der versucht hat, in die infizierte Datei im freigegebenen Ordner zu schreiben oder daraus zu lesen.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Berichtseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Berichte**, um die Protokollierungsaktivitäten zu konfigurieren und festzulegen, welche Daten Sie für die einzelnen Protokolleinträge erfassen möchten.

HINWEIS
Die Protokolldatei ist ein wichtiges Verwaltungstool, mit dem Sie Virenaktivitäten im Netzwerk verfolgen und die vom Scanner zur Erkennung und Behandlung erkannter Viren verwendeten Einstellungen festhalten können. Anhand der in der Datei protokollierten Ereignisse können Sie feststellen, welche Dateien durch Sicherungskopien ersetzt, im Quarantäneordner geprüft oder vom Rechner gelöscht werden müssen. Weitere Informationen zum Anzeigen des Protokolls finden Sie unter *Anzeigen des Aktivitätsprotokolls* auf Seite 88.

So konfigurieren Sie die **Berichts**eigenschaften:

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Allgemeine Einstellungen**.

2 Wählen Sie die Registerkarte **Berichte**.



Abbildung 3-5. Allgemeine Einstellungen – Registerkarte "Berichte"

3 Wählen Sie unter **Protokolldatei** eine dieser Optionen:

- **In Datei protokollieren**: *Diese Option ist standardmäßig ausgewählt.* Virusaktivitäten werden beim Scannen bei Zugriff in einer Protokolldatei aufgezeichnet.
- Sie können den im Textfeld angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einer anderen geeigneten Datei auf dem Computer oder im Netzwerk zu wechseln.

  HINWEIS
  Standardmäßig schreibt der Scanner Protokollinformationen in die Datei ONACCESSSCANLOG.TXT in diesem Ordner:

  ```
  <Laufwerk>:Winnt\Profiles\All Users\Application
  Data\Network Associates\VirusScan
  ```

- **Größe begrenzen auf**: *Diese Option ist standardmäßig ausgewählt. Die Standardgröße der Protokolldatei ist 1 MB.* Übernehmen Sie die Standardgröße oder legen Sie einen anderen Wert für die Protokolldatei fest. Wenn Sie diese Option auswählen, geben Sie einen Wert zwischen 1 MB und 999 MB ein.

  HINWEIS
  Wenn die Datenmenge in der Protokolldatei die von Ihnen festgelegte Dateigröße übersteigt, werden 20 Prozent der Protokolldateieinträge (die ältesten) gelöscht und der Datei neue Daten hinzugefügt.

4 Legen Sie unter **Zusätzlich zur Virusaktivität zu protokollierende Aktionen** fest, welche zusätzlichen Informationen in der Protokolldatei aufgezeichnet werden sollen:

- **Sitzungseinstellungen**: In der Protokolldatei werden die für die einzelnen Scan-Sitzungen ausgewählten Eigenschaften erfasst.

  HINWEIS
  Eine Scan-Sitzung entspricht der Zeitspanne, die der Scanner nach dem Laden im Speicher des Computers verbleibt. Diese Zeitspanne endet, wenn Sie das Programm beenden oder den Computer neu starten.

- **Sitzungszusammenfassung** *Diese Option ist standardmäßig ausgewählt.* Die Aktionen des Scanners bei den einzelnen Scan-Sitzungen werden zusammengefasst und der Protokolldatei hinzugefügt. Zu den Zusammenfassungsinformationen gehören die Anzahl der gescannten Dateien, Anzahl und Typ der entdeckten Viren, die Anzahl der verschobenen, gelöschten oder bereinigten Dateien sowie weitere Informationen.

- **Fehler beim Scannen verschlüsselter Dateien** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden die Namen der verschlüsselten Dateien erfasst, die nicht gescannt werden konnten.

- **Benutzername** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei wird der Name des Benutzers erfasst, der zum Zeitpunkt der Aufzeichnung der jeweiligen Protokolleinträge auf dem Computer angemeldet war.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Vorgangseinstellungen

Geben Sie an, ob die gleichen Einstellungen für alle Vorgänge verwendet werden oder ob unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem und hohem Risiko angegeben werden sollen.

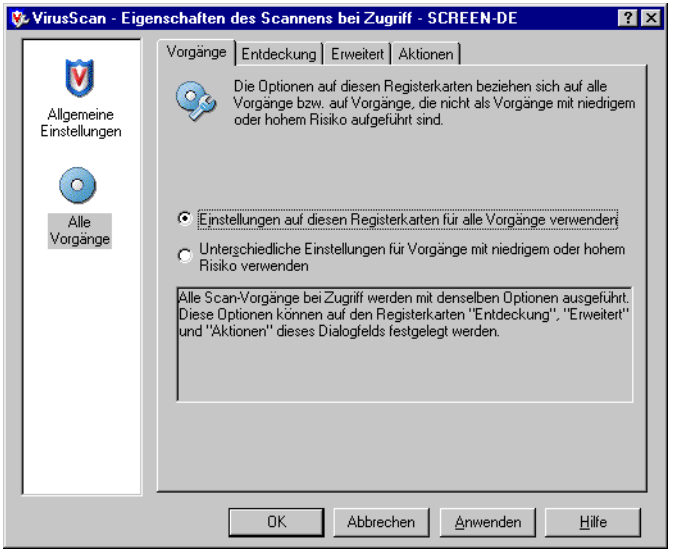

VirusScan - Eigenschaften des Scannens bei Zugriff - SCREEN-DE
Allgemeine Einstellungen
Alle Vorgänge
Vorgänge
Entdeckung
Erweitert
Aktionen
Die Optionen auf diesen Registerkarten beziehen sich auf alle Vorgänge bzw. auf Vorgänge, die nicht als Vorgänge mit niedrigem oder hohem Risiko aufgeführt sind.
Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden
Unterschiedliche Einstellungen für Vorgänge mit niedrigem oder hohem Risiko verwenden
Alle Scan-Vorgänge bei Zugriff werden mit denselben Optionen ausgeführt. Diese Optionen können auf den Registerkarten "Entdeckung", "Erweitert" und "Aktionen" dieses Dialogfelds festgelegt werden.
OK
Abbrechen
Anwenden
Hilfe

Abbildung 3-6. Eigenschaften des Scannens bei Zugriff – Alle Vorgänge

- **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden**: Geben Sie die gleichen Scan-Eigenschaften für alle Vorgänge an. Die Vorgehensweise für die Festlegung von Eigenschaften für alle Vorgänge entspricht der Vorgehensweise für die Festlegung von Eigenschaften für Standardvorgänge. Siehe *Standardvorgänge* auf Seite 57 für eine schrittweise Anleitung.
- **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden**: Geben Sie unterschiedliche Eigenschaften für Vorgänge an, je nachdem, ob es sich um Standardvorgänge oder um Vorgänge mit geringem oder hohem Risiko handelt. Weitere Informationen finden Sie unter *Vorgänge mit geringem und hohem Risiko* auf Seite 67.

HINWEIS

Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

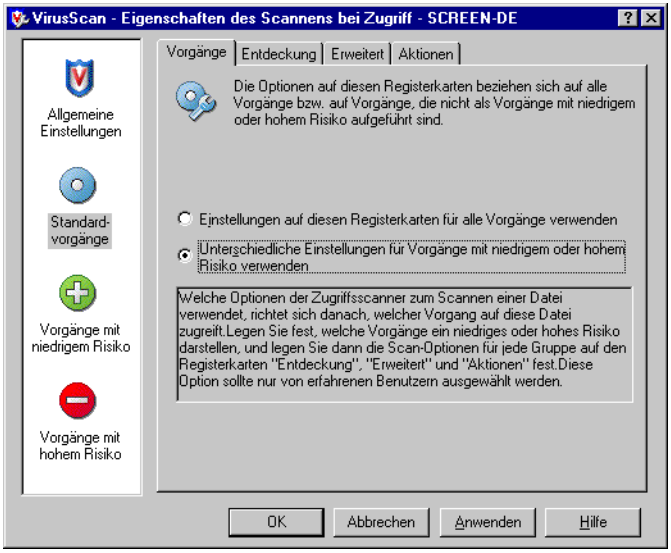

VirusScan - Eigenschaften des Scannens bei Zugriff - SCREEN-DE
Allgemeine Einstellungen
Standard-vorgänge
Vorgänge mit niedrigem Risiko
Vorgänge mit hohem Risiko
Vorgänge
Entdeckung
Erweitert
Aktionen
Die Optionen auf diesen Registerkarten beziehen sich auf alle Vorgänge bzw. auf Vorgänge, die nicht als Vorgänge mit niedrigem oder hohem Risiko aufgeführt sind.
Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden
Unterschiedliche Einstellungen für Vorgänge mit niedrigem oder hohem Risiko verwenden
Welche Optionen der Zugriffsscanner zum Scannen einer Datei verwendet, richtet sich danach, welcher Vorgang auf diese Datei zugreift. Legen Sie fest, welche Vorgänge ein niedriges oder hohes Risiko darstellen, und legen Sie dann die Scan-Optionen für jede Gruppe auf den Registerkarten "Entdeckung", "Erweitert" und "Aktionen" fest. Diese Option sollte nur von erfahrenen Benutzern ausgewählt werden.
OK
Abbrechen
Anwenden
Hilfe

Abbildung 3-7. Eigenschaften des Scannens bei Zugriff

In diesem Abschnitt werden die folgenden Themen erläutert:

- Standardvorgänge
- Vorgänge mit geringem und hohem Risiko

Standardvorgänge

Ein Standardvorgang ist jeder Vorgang, der nicht als Vorgang mit geringem oder hohem Risiko definiert ist.

> **HINWEIS**
> Folgen Sie für die Einstellung von Eigenschaften für alle Vorgänge der Anleitung für die Einstellung der Eigenschaften für Standardvorgänge.

Diese Eigenschaften können konfiguriert werden:

- Vorgangseigenschaften
- Erkennungseigenschaften
- Erweiterte Eigenschaften
- Aktionseigenschaften

Vorgangseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Vorgänge**, um Eigenschaften für Standardvorgänge oder alle Vorgänge anzugeben:

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.
2. Wählen Sie die Registerkarte **Vorgänge** aus, wenn sie nicht bereits ausgewählt ist und wählen Sie dann eine der folgenden Optionen aus:
   - **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden**: *Diese Option ist standardmäßig ausgewählt.* Wenn Sie Eigenschaften angeben, wenn diese Option ausgewählt ist, gelten die ausgewählten Eigenschaften für alle Prozesse. Es ist nicht möglich, unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko festzulegen.
   - **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden**: Legen Sie jeweils unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko fest.

     HINWEIS
     Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

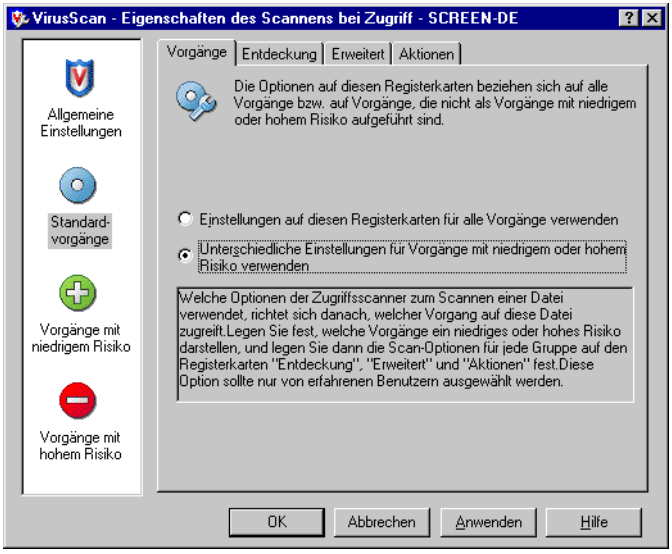

VirusScan - Eigenschaften des Scannens bei Zugriff - SCREEN-DE
Allgemeine Einstellungen
Standard-vorgänge
Vorgänge mit niedrigem Risiko
Vorgänge mit hohem Risiko
Vorgänge
Entdeckung
Erweitert
Aktionen
Die Optionen auf diesen Registerkarten beziehen sich auf alle Vorgänge bzw. auf Vorgänge, die nicht als Vorgänge mit niedrigem oder hohem Risiko aufgeführt sind.
Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden
Unterschiedliche Einstellungen für Vorgänge mit niedrigem oder hohem Risiko verwenden
Welche Optionen der Zugriffsscanner zum Scannen einer Datei verwendet, richtet sich danach, welcher Vorgang auf diese Datei zugreift. Legen Sie fest, welche Vorgänge ein niedriges oder hohes Risiko darstellen, und legen Sie dann die Scan-Optionen für jede Gruppe auf den Registerkarten "Entdeckung", "Erweitert" und "Aktionen" fest. Diese Option sollte nur von erfahrenen Benutzern ausgewählt werden.
OK
Abbrechen
Anwenden
Hilfe

Abbildung 3-8. Standardvorgänge – Registerkarte "Vorgänge"

3. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erkennungseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erkennung**, um festzulegen, welche Dateitypen beim Scannen bei Zugriff zu welchem Zeitpunkt überprüft werden.

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.

2. Wählen Sie eine der folgenden Optionen aus:

   - **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden**: *Diese Option ist standardmäßig ausgewählt.* Wenn Sie Eigenschaften angeben, wenn diese Option ausgewählt ist, gelten die ausgewählten Eigenschaften für alle Prozesse. Es ist nicht möglich, unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko festzulegen.

   - **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden**: Legen Sie jeweils unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko fest.

     HINWEIS
     Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

3. Wählen Sie die Registerkarte **Erkennung**.

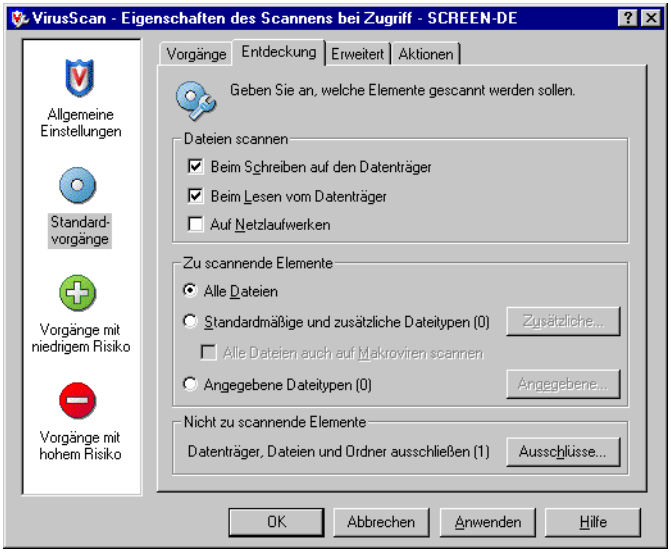


Abbildung 3-9. Standardvorgänge – Registerkarte "Erkennung"

4 Wählen Sie unter **Dateien scannen** eine beliebige Kombination der folgenden Scan-Optionen aus:

- **Beim Schreiben auf den Datenträger**: *Diese Option ist standardmäßig ausgewählt.* Es werden alle Dateien gescannt, die auf dem Server, der Arbeitsstation oder anderen Datenspeichergeräten gespeichert oder geändert werden.
- **Beim Lesen vom Datenträger**: *Diese Option ist standardmäßig ausgewählt.* Es werden alle Dateien gescannt, die vom Server, der Arbeitsstation oder anderen Datenspeichergeräten gelesen werden.
- **Auf Netzlaufwerken**: Netzwerkressourcen werden in Scan-Vorgänge bei Zugriff einbezogen. So kann der Virusschutz bequem ausgeweitet werden.

  HINWEIS
  Die Aufnahme von Netzwerkressourcen könnte eine negative Auswirkung auf die Gesamtleistung des Systems haben, auf dem der Scan ausgeführt wird.

  WARNUNG
  Wenn Sie eine Datei von einem Computer auf einen anderen kopieren oder verschieben und die Eigenschaften für das Scannen bei Zugriff auf beiden Computern so konfiguriert wurden, dass Dateien sowohl beim Lesen von der Festplatte als auch beim Schreiben auf die Festplatte gescannt werden, erfolgt der Scan jeweils beim Lesen durch den *Ursprungscomputer* sowie beim Schreiben auf den *Zielcomputer*.

  Wenn das vorherrschende Verkehrsmuster in Ihrem Netzwerk im Kopieren oder Verschieben von Dateien von einem Computer auf einen anderen besteht, kann es sinnvoll sein, die Scan-Eigenschaften so zu konfigurieren, dass nur Dateien gescannt werden, die auf Festplatten geschrieben werden, aber keine Dateien, die von Festplatten gelesen werden. Dadurch wird ein doppeltes Scannen der einzelnen Dateien vermieden. Sie können dasselbe Ergebnis erzielen, wenn alle Computer so konfiguriert werden, dass keine geschriebenen, sondern nur gelesene Dateien gescannt werden.

  Wenn Sie eines dieser Konfigurationsmuster verwenden, ist es wichtig, dass *alle Computer identisch konfiguriert werden*. Wählen Sie keine Konfiguration, bei der einige Computer nur Dateien scannen, die auf Festplatte geschrieben werden und andere nur Dateien scannen, die von Festplatten gelesen werden. Bei einer solchen Konfiguration könnte eine infizierte Datei von einem Computer, der nur Dateien scannt, die auf Festplatte geschrieben werden, auf einen Computer kopiert werden, der nur Dateien scannt, die von der Festplatte gelesen werden.

5 Wählen Sie unter **Zu scannende Elemente** eine der folgenden Optionen:

- **Alle Dateien**: *Diese Option ist standardmäßig ausgewählt.* Alle Dateien (unabhängig von der Erweiterung) werden gescannt.
- **Standardmäßige und zusätzliche Dateitypen**: Die standardmäßig aufgelisteten Erweiterungen und alle zusätzlich angegebenen Dateitypen werden gescannt. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert. Sie können benutzerdefinierte Dateityperweiterungen hinzufügen und entfernen, aber keine Dateityperweiterungen aus der Standardliste löschen. Sie können in der Standardliste vorhandene Erweiterungen auch ausschließen. Weitere Informationen finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.
  - **Ergänzungen**: Klicken Sie bei Auswahl von **Standardmäßige und zusätzliche Dateitypen** auf **Ergänzungen**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen von Dateityperweiterungen* auf Seite 75.

    Der Zugriffsscanner kann maximal 1.000 zusätzliche Erweiterungen auflisten.
  - **Alle Dateien auch auf Makroviren scannen**: Alle Dateien werden unabhängig von der Erweiterung auf Makroviren gescannt. Diese Option ist nur verfügbar, wenn die Option **Standardmäßige und zusätzliche Dateitypen** aktiviert ist.

    HINWEIS
    Ein Scan auf Makroviren in allen Dateien könnte die Leistungsfähigkeit beeinträchtigen.
- **Angegebene Dateitypen**: Nur die von Ihnen angegebenen Dateitypen werden gescannt.
  - **Angegebene**: Klicken Sie bei Auswahl von **Angegebene Dateitypen** auf **Angegebene**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Die Liste der Dateityperweiterungen kann auch als Standardliste definiert werden. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen benutzerdefinierter Dateityperweiterungen* auf Seite 76.

    Der Zugriffsscanner kann maximal 1.000 angegebene Erweiterungen auflisten.

6 Klicken Sie unter **Nicht zu scannende Elemente** auf **Ausschlüsse**, um die Dateien, Ordner und Laufwerke anzugeben, die nicht gescannt werden sollen. Ausführliche Anweisungen dazu finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erweiterte Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erweitert**, um erweiterte Scan-Optionen für Heuristik, Nicht-Viren-Programmdateien und komprimierte Dateien festzulegen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.

2 Wählen Sie eine der folgenden Optionen aus:

- **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden**: *Diese Option ist standardmäßig ausgewählt.* Wenn Sie Eigenschaften angeben, wenn diese Option ausgewählt ist, gelten die ausgewählten Eigenschaften für alle Prozesse. Es ist nicht möglich, unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko festzulegen.
- **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden**: Legen Sie jeweils unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko fest.

  HINWEIS
  Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

3 Wählen Sie die Registerkarte **Erweitert** aus.

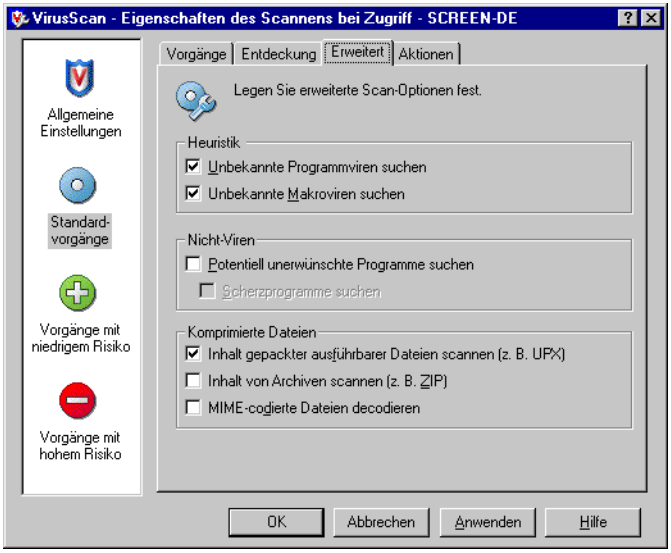


Abbildung 3-10. Standardvorgänge – Registerkarte "Erweitert"

4 Geben Sie unter **Heuristik** an, ob der Scanner die Wahrscheinlichkeit bewerten soll, mit der es sich bei unbekanntem Code oder Microsoft Office-Makros um Viren handelt. Wenn diese Funktion aktiviert ist, analysiert der Scanner, wie wahrscheinlich es ist, dass es sich bei dem Code um Varianten bekannter Viren handelt. Wählen Sie eine beliebige Kombination dieser Optionen:

- **Unbekannte Programmviren suchen**: *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt*. Ausführbare Dateien mit virenähnlichem Code werden wie infizierte Dateien behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion an.

- **Unbekannte Makroviren suchen**: *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt*. Eingebettete Makros mit virenähnlichem Code werden wie infizierte Makros behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion an.

  HINWEIS
  Diese Option ist nicht mit der Option **Alle Dateien auch auf Makroviren scannen** auf der Registerkarte **Erkennung** identisch, mit der der Scanner nach allen bekannten Makroviren sucht. Mit dieser Option wird der Scanner angewiesen, die *Wahrscheinlichkeit* zu bewerten, mit der es sich bei einem unbekannten Makro um ein Virus handelt.

5 Geben Sie unter **Nicht-Viren** an, ob der Scanner nach potenziell unerwünschten Nicht-Viren-Anwendungen suchen soll.

- **Potenziell unerwünschte Programme suchen**: Potenziell unerwünschte Programme werden erkannt.

  - **Scherzviren suchen**: Wenn Sie die Option **Potenziell unerwünschte Programme suchen** gewählt haben, können Sie auch nach Scherzprogrammen suchen.

    WARNUNG
    VirusScan Enterprise unternimmt keine Maßnahmen gegen potenziell unerwünschte Programmdateien oder Scherzprogramme, die entdeckt werden. Erkennungen werden in der Protokolldatei protokolliert.

    Wenn Sie bei einer erkannten, potenziell unerwünschten Programmdatei oder einem Scherzprogramm aktiv werden möchten, müssen Sie dies manuell tun. Wenn Sie z. B. ein erkanntes Scherzprogramm entfernen möchten, müssen Sie es manuell entfernen.

6 Wählen Sie unter **Komprimierte Dateien** aus, welche Typen von komprimierten Dateien vom Scanner überprüft werden sollen:

- **Inhalt gepackter ausführbarer Dateien scannen.** *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt*. Komprimierte Dateien mit ausführbaren Programmdateien werden überprüft. Eine verpackte Programmdatei wird beim Ausführen niemals auf einen Datenträger, sondern immer direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.
- **Inhalt von Archiven scannen**: Archivdateien und ihr Inhalt werden überprüft. Eine Archivdatei ist eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann. Die in Archiven enthaltenen Dateien werden gescannt, bevor Sie auf Datenträgern gespeichert werden.
- **MIME-codierte Dateien decodieren**: Multipurpose Internet Mail Extensions-(MIME) kodierte Dateien werden erkannt, dekodiert und dann gescannt.

  HINWEIS
  Das Scannen komprimierter Dateien verbessert zwar den Schutz, dafür kann sich jedoch auch die für den Scan-Vorgang benötigte Zeit erhöhen.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Aktionseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Aktionen**, um die primären und sekundären Aktionen festzulegen, die beim Erkennen eines Virus vom Scan-Programm ausgeführt werden sollen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.

2 Wählen Sie eine der folgenden Optionen aus:

- **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden**: *Diese Option ist standardmäßig ausgewählt.* Wenn Sie Eigenschaften angeben, wenn diese Option ausgewählt ist, gelten die ausgewählten Eigenschaften für alle Prozesse. Es ist nicht möglich, unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko festzulegen.
- **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden**: Legen Sie jeweils unterschiedliche Einstellungen für Standardvorgänge und Vorgänge mit geringem bzw. mit hohem Risiko fest.

  HINWEIS
  Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

3 Wählen Sie die Registerkarte **Aktionen**.


VirusScan - Eigenschaften des Scannens bei Zugriff - SCREEN-DE
Allgemeine Einstellungen
Standard-vorgänge
Vorgänge mit niedrigem Risiko
Vorgänge mit hohem Risiko
Vorgänge
Entdeckung
Erweitert
Aktionen
Legen Sie fest, wie VirusScan bei Entdeckung eines Virus reagieren soll.
Wenn ein Virus gefunden wird:
Infizierte Dateien automatisch säubern
Mit dieser Option werden infizierte Dateien von VirusScan automatisch gesäubert.
Wenn die oben genannte Aktion fehlschlägt:
Infizierte Dateien in Ordner verschieben
Mit dieser Option legen Sie fest, dass VirusScan alle infizierten Dateien automatisch in den Quarantäneordner verschiebt.
Den Speicherort des Quarantäneordners legen Sie auf der Registerkarte "Allgemein" unter "Allgemeine Einstellungen" fest.
OK
Abbrechen
Anwenden
Hilfe

Abbildung 3-11. Standardvorgänge – Registerkarte "Aktionen"

4 Wählen Sie unter **Wenn ein Virus gefunden wird** die primäre Aktion aus, die das Scan-Programm ausführen soll, wenn ein Virus gefunden wird.

> **HINWEIS**
> Die primäre Standardaktion ist **Infizierte Dateien automatisch säubern**.

Klicken Sie auf ▼, um eine dieser Aktionen auszuwählen:

- **Zugriff auf infizierte Dateien verweigern** Allen Benutzern wird der Zugriff auf vom Scanner gefundene infizierte Dateien verweigert. Denken Sie daran, unter **Allgemeine Einstellungen** auf der Registerkarte **Berichte** die Eigenschaft **In Datei protokollieren** zu aktivieren, damit aufgezeichnet wird, welche Dateien infiziert sind.

  > **HINWEIS**
  > Wenn die Datei von einer externen Quelle, z. B. CD-ROM oder Internet, auf das lokale System geschrieben wird, fügt der Scanner am Ende des Dateinamens die Erweiterung .VIR hinzu. Der Scanner betrachtet diese Art der Dateiaktion als *Schreib*aktion.
  >
  > Wenn die Datei z. B. von einem Speicherort auf der Festplatte an einen anderen Speicherort kopiert wird, wird die Erweiterung .VIR nicht dem Dateinamen hinzugefügt. Der Scanner betrachtet dies als *Verschiebe*aktion.

- **Infizierte Dateien in Ordner verschieben**: Der Scanner verschiebt infizierte Dateien in einen Ordner, der standardmäßig mit *quarantine* benannt ist. Sie können unter **Allgemeine Einstellungen** auf der Registerkarte **Allgemein** im Textfeld **Quarantäneordner** den Namen des Ordners ändern.

- **Infizierte Dateien automatisch löschen** Der Scanner löscht infizierte Dateien sofort nach dem Entdecken. Denken Sie daran, unter **Allgemeine Einstellungen** auf der Registerkarte **Berichte** die Eigenschaft **In Datei protokollieren** zu aktivieren, damit aufgezeichnet wird, welche Dateien infiziert sind.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

  WARNUNG
  Wenn Sie auf der Registerkarte **Erweitert** die Option **Unbekannte Makroviren suchen** ausgewählt haben, wird die hier von Ihnen festgelegte Aktion auf alle Makros mit virenähnlichem Code angewendet. Bei Auswahl der Option **Infizierte Dateien automatisch löschen** werden alle Dateien mit Code, der Makroviren ähnelt, und alle Archive, die eine infizierte Datei enthalten, gelöscht. Wenn Sie das nicht beabsichtigen, sollten Sie sicherstellen, dass die von Ihnen getroffene Auswahl an Aktionen der für Makros getroffenen Auswahl an Aktionen entspricht.

- **Infizierte Dateien automatisch säubern**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner versucht, den Virus aus der infizierten Datei zu entfernen. Wenn der Scanner den Virus nicht entfernen kann oder der Virus die Datei irreparabel beschädigt hat, führt der Scanner die sekundäre Aktion aus. Weitere Informationen finden Sie unter Schritt 5.

5 Wählen Sie unter **Wenn die oben genannte Aktion fehlschlägt** die sekundäre Aktion aus, die das Scan-Programm beim Fehlschlagen der primären Aktion ausführen soll. Welche Optionen hierfür verfügbar sind, hängt von der Auswahl der primären Aktion ab.

  HINWEIS
  Bei der sekundären Standardaktion handelt es sich um **Infizierte Dateien in Ordner verschieben**.

  Klicken Sie auf  , um die sekundäre Aktion auszuwählen:

  - **Zugriff auf infizierte Dateien verweigern**
  - **Infizierte Dateien in Ordner verschieben**: *Diese Option ist standardmäßig ausgewählt.*

- **Infizierte Dateien automatisch löschen**

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

6. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Vorgänge mit geringem und hohem Risiko

Mit dem vorgangsbasierten Scannen können Sie Scan-Richtlinien definieren, die auf dem wahrgenommenen Infektionsrisiko aus einem definierten Vorgang beruhen.

Legen Sie fest, welche Vorgänge als geringes oder hohes Risiko eingestuft werden sollen, und stellen Sie dann die Eigenschaften für jeden Vorgangstyp ein.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Zuordnen eines Risikos zu einem Vorgang
- Vorgangseigenschaften
- Erkennungseigenschaften
- Erweiterte Eigenschaften
- Aktionseigenschaften

Zuordnen eines Risikos zu einem Vorgang

Ein Vorgang ist ein Programm, das sich in Ausführung befindet. Ein Programm kann einen oder mehrere Vorgänge auslösen. Wenn Sie festlegen, welches Risiko bzw. welche Scan-Richtlinien einem Vorgang zugewiesen werden sollen, sollten Sie bedenken, dass die Scan-Richtlinien nur für die untergeordneten Vorgänge des definierten übergeordneten Vorgangs gelten. Beispiel: Wenn Sie die ausführbare Datei von Microsoft Word, WINWORD.EXE, als Scan-Vorgang mit hohem Risiko definieren, werden alle Microsoft Word-Dokumente, auf die zugegriffen wird, gemäß der Scan-Richtlinien für hohes Risiko gescannt. Die Datei WINWORD.EXE würde jedoch beim Start von Microsoft Word, dem übergeordneten Vorgang, gemäß der Richtlinie für den Vorgang gescannt, der die Datei gestartet hat.

Sie können Vorgängen zwei Arten von Risiken zuordnen:

- *Vorgänge mit geringem Risiko* sind als die Vorgänge definiert, die eine geringere Wahrscheinlichkeit einer Infizierung mit sich bringen. Das können Vorgänge sein, die auf viele Dateien zugreifen, aber auf eine Weise, dass nur ein geringes Risiko der Virusverbreitung besteht. Einige Beispiele:

  - Backup-Software
  - Kompilierungsvorgänge

- *Vorgänge mit hohem Risiko* sind als die Vorgänge definiert, die eine höhere Wahrscheinlichkeit einer Infizierung mit sich bringen. Einige Beispiele:
  - Vorgänge, die andere Vorgänge auslösen, beispielsweise Microsoft Windows-Explorer oder die Eingabeaufforderung
  - Vorgänge für die Ausführung, beispielsweise WINWORD oder CSCRIPT.
  - Vorgänge für das Herunterladen aus dem Internet, beispielsweise Browser, Instant Messenger und Mail-Clients

    HINWEIS
    Wenn Sie VirusScan Enterprise mit den Standardeinstellungen installieren, ist die Option **Einstellungen auf diesen Registerkarten für alle Vorgänge verwenden** ausgewählt. Wenn Sie **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden** auswählen, werden einige Vorgänge als Vorgänge mit hohem Risiko vordefiniert. Sie können diese Liste Ihren Anforderungen entsprechend anpassen.

Jeder Vorgang, der weder als niedriges noch als hohes Risiko eingestuft ist, wird als *Standardvorgang* betrachtet und mit den Eigenschaften gescannt, die Sie für Standardvorgänge festgelegt haben.

Gehen Sie folgendermaßen vor, um zu bestimmen, welchem Vorgang welches Risiko zugeordnet werden soll:

1. Bestimmen Sie, warum unterschiedliche Scan-Richtlinien gelten sollen. Die beiden häufigsten Gründe beim Abwägen von Leistungsaspekten und Risiko sind folgende:
   - Bestimmte Vorgänge, beispielsweise Downloads aus dem Web, sollen gründlicher gescannt werden, als bei den standardmäßigen Scan-Richtlinien der Fall.
   - Bestimmte Vorgänge sollen weniger gründlich gescannt werden, je nach Risiko und Leistungsbeeinträchtigung durch das Scannen. Das Protokollieren von Streaming Media wie etwas Videos weist ein sehr geringes Risiko auf, ist jedoch sehr ressourcenintensiv.
2. Entscheiden Sie, welche Vorgänge ein geringes und welche Vorgänge ein hohes Risiko darstellen. Bestimmen Sie zunächst, welches Programm für den jeweiligen Vorgang zuständig ist, und ermitteln Sie dann, welches Risiko welchem Vorgang zugeordnet ist. Verwenden Sie den Windows Task-Manager oder Windows-Systemmonitor, um herauszufinden, welche Vorgänge am meisten CPU-Zeit und am meisten Arbeitsspeicher benötigen. Sobald Sie über diese Informationen verfügen, können Sie jedem Vorgang, je nach Leistung und Risiko für diesen Vorgang, eine Scan-Richtlinie zuordnen.
3. Konfigurieren Sie die Scan-Richtlinien für jede der drei Stufen: Standard, hohes Risiko und geringes Risiko.

HINWEIS
Es wird davon abgeraten, die Scan-Ebene für Vorgänge mit hohem Risiko herabzusetzen. Die Scan-Richtlinien für hohes Risiko sind ursprünglich genauso festgelegt wie die für Standardvorgänge, um zu gewährleisten, dass Vorgänge mit hohem Risiko gründlich gescannt werden.

Vorgangseigenschaften

Verwenden Sie die Option der Registerkarte **Vorgänge**, um Vorgänge als geringes bzw. hohes Risiko einzustufen:

HINWEIS
Jeder Vorgang, der weder als niedriges noch als hohes Risiko eingestuft ist, wird als Standardvorgang betrachtet und mit den Eigenschaften gescannt, die Sie für Standardvorgänge festgelegt haben.

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.
2. Wählen Sie **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden** aus.

   HINWEIS
   Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.
3. Wählen Sie **Vorgänge mit geringem Risiko** oder **Vorgänge mit hohem Risiko** aus.
4. Wählen Sie die Registerkarte **Vorgänge** aus.

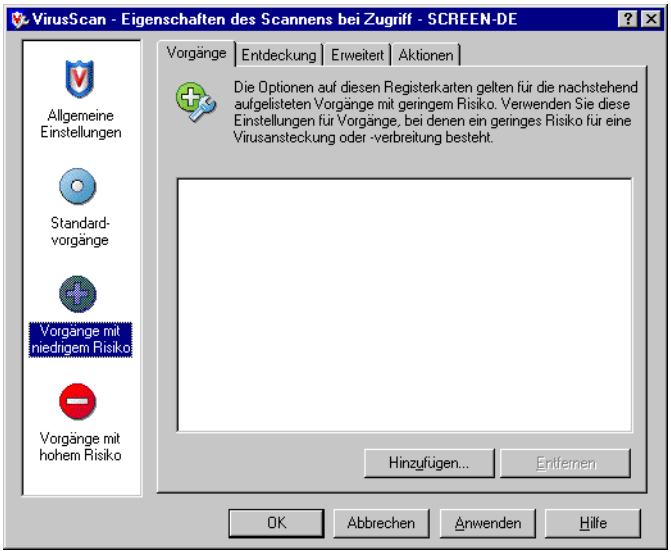


Abbildung 3-12. Vorgänge mit geringem oder hohem Risiko – Registerkarte "Vorgänge"

Die Liste enthält eine nach Dateinamen alphabetisch sortierte Auflistung der aktuellen Vorgänge. Jeder Vorgang wird mit seinem Anwendungssymbol, dem Dateinamen und ggf. einer Beschreibung angezeigt. Die Standardeinstellungen sind:

- Die Liste **Vorgänge mit geringem Risiko** ist leer.
- *D*ie Liste **Vorgänge mit hohem Risiko** enthält Vorgänge, die McAfee Security als hohes Risiko einstuft. Sie können dieser Liste entsprechend Ihren Sicherheitsanforderungen Vorgänge hinzufügen oder sie entfernen.

  HINWEIS
  Die Schritte, die Sie zum Hinzufügen oder Auswählen von Vorgängen ausführen, sind für Vorgänge mit geringem bzw. hohem Risiko identisch.

5 Klicken Sie zum Hinzufügen von Anwendungen auf die Schaltfläche **Hinzufügen**. Das Dialogfeld **Anwendung auswählen** wird angezeigt.


Anwendung auswählen
Wählen Sie die Anwendung aus, die zur Liste hinzugefügt werden soll. Wenn die gewünschte Anwendung nicht aufgelistet ist, klicken Sie auf "Durchsuchen".
Artgalry.exe (Clip Gallery 5.0 OLE Server)
Cag.exe (Clip Gallery 5.0 Helper Application)
Cdplayer.exe (CD-Spieler)
Clipbrd.exe (Windows NT-Ablagemappe)
Conf.exe (Windows® NetMeeting®)
Esserver.exe (COM+ EventSystem Service)
Exchng32.exe (Microsoft Exchange EXE)
Explorer.exe (Windows-Explorer)
Finder.exe (Microsoft Outlook Item Finder)
OK
Abbrechen
Durchsuchen...

Abbildung 3-13. Anwendung auswählen

a Wählen Sie die Anwendung(en), die Sie hinzufügen möchten, mithilfe der folgenden Methoden aus:

- Wählen Sie eine oder mehrere Anwendungen in der Liste aus.

  Mit der Tastenkombination STRG + UMSCHALTTASTE können Sie mehrere Anwendungen auswählen.

- Klicken Sie auf **Durchsuchen**, um innerhalb des Netzwerks nach einer Anwendung zu suchen.

b Wenn Sie alle gewünschten Anwendungen ausgewählt haben, klicken Sie auf **OK**, um die von Ihnen getroffene Auswahl zu speichern und zur Registerkarte **Vorgänge** zurückzukehren.

6 Sie können Anwendungen entfernen, indem Sie eine oder mehrere Anwendungen in der Liste markieren und anschließend auf **Entfernen** klicken.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

8 Wiederholen Sie Schritt 3 bis Schritt 7, um Anwendungen als geringes oder hohes Risiko einzustufen.

Erkennungseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erkennung**, um festzulegen, welche Dateitypen beim Scannen bei Zugriff zu welchem Zeitpunkt überprüft werden.

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.
2. Wählen Sie **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden** aus.

   HINWEIS
   Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.
3. Wählen Sie **Vorgänge mit geringem Risiko** oder **Vorgänge mit hohem Risiko** aus.
4. Wählen Sie die Registerkarte **Erkennung**.

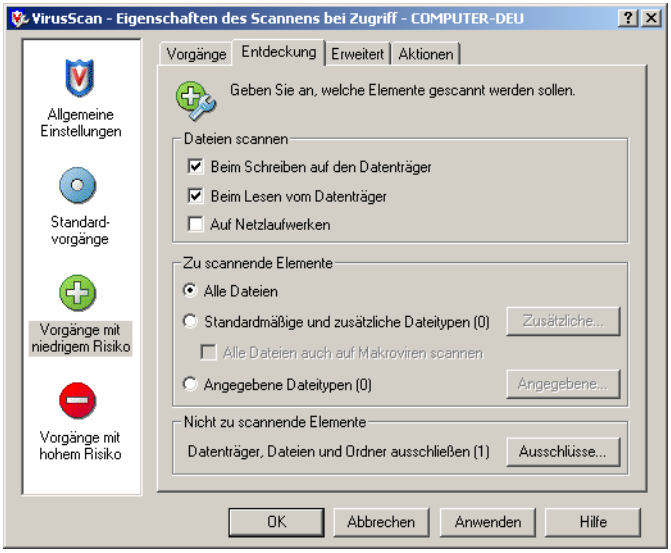


Abbildung 3-14. Vorgänge mit geringem oder hohem Risiko – Registerkarte "Erkennung"

HINWEIS
Nachdem Sie das Vorgangssymbol im linken Bereich ausgewählt haben, sind die weiteren Schritte zur Festlegung von Optionen für die **Erkennung** für Vorgänge mit geringem oder hohem Risiko identisch.

5 Wählen Sie unter **Dateien scannen** eine beliebige Kombination der folgenden Scan-Optionen aus:

- **Beim Schreiben auf den Datenträger**: *Diese Option ist standardmäßig ausgewählt.* Es werden alle Dateien gescannt, die auf dem Server, der Arbeitsstation oder anderen Datenspeichergeräten gespeichert oder geändert werden.
- **Beim Lesen vom Datenträger**: *Diese Option ist standardmäßig ausgewählt.* Es werden alle Dateien gescannt, die vom Server, der Arbeitsstation oder anderen Datenspeichergeräten gelesen werden.
- **Auf Netzlaufwerken**: Netzwerkressourcen werden in Scan-Vorgänge bei Zugriff einbezogen. So kann der Virusschutz bequem ausgeweitet werden.

  HINWEIS
  Die Aufnahme von Netzwerkressourcen könnte eine negative Auswirkung auf die Gesamtleistung des Systems haben, auf dem der Scan ausgeführt wird.

  WARNUNG
  Wenn Sie eine Datei von einem Computer auf einen anderen kopieren oder verschieben und die Eigenschaften für das Scannen bei Zugriff auf beiden Computern so konfiguriert wurden, dass Dateien sowohl beim Lesen von der Festplatte als auch beim Schreiben auf die Festplatte gescannt werden, erfolgt der Scan jeweils beim Lesen durch den *Ursprungscomputer* sowie beim Schreiben auf den *Zielcomputer*.

  Wenn das vorherrschende Verkehrsmuster in Ihrem Netzwerk im Kopieren oder Verschieben von Dateien von einem Computer auf einen anderen besteht, kann es sinnvoll sein, die Scan-Eigenschaften so zu konfigurieren, dass nur Dateien gescannt werden, die auf Festplatten geschrieben werden, aber keine Dateien, die von Festplatten gelesen werden. Dadurch wird ein doppeltes Scannen der einzelnen Dateien vermieden. Sie können dasselbe Ergebnis erzielen, wenn alle Computer so konfiguriert werden, dass keine geschriebenen, sondern nur gelesene Dateien gescannt werden.

  Wenn Sie eines dieser Konfigurationsmuster verwenden, ist es wichtig, dass *alle Computer identisch konfiguriert werden*. Wählen Sie keine Konfiguration, bei der einige Computer nur Dateien scannen, die auf Festplatte geschrieben werden und andere nur Dateien scannen, die von Festplatten gelesen werden. Bei einer solchen Konfiguration könnte eine infizierte Datei von einem Computer, der nur Dateien scannt, die auf Festplatte geschrieben werden, auf einen Computer kopiert werden, der nur Dateien scannt, die von der Festplatte gelesen werden.

6 Wählen Sie unter **Zu scannende Elemente** eine der folgenden Optionen:

- **Alle Dateien**: *Diese Option ist standardmäßig ausgewählt.* Alle Dateien (unabhängig von der Erweiterung) werden gescannt.
- **Standardmäßige und zusätzliche Dateitypen**: Die standardmäßig aufgelisteten Erweiterungen und alle zusätzlich angegebenen Dateitypen werden gescannt. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert. Sie können benutzerdefinierte Dateityperweiterungen hinzufügen und entfernen, aber keine Dateityperweiterungen aus der Standardliste löschen. Sie können in der Standardliste vorhandene Erweiterungen auch ausschließen. Weitere Informationen finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.
  - **Ergänzungen**: Klicken Sie bei Auswahl von **Standardmäßige und zusätzliche Dateitypen** auf **Ergänzungen**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen von Dateityperweiterungen* auf Seite 75.

    Der Zugriffsscanner kann maximal 1.000 zusätzliche Erweiterungen auflisten.
  - **Alle Dateien auch auf Makroviren scannen**: Alle Dateien werden unabhängig von der Erweiterung auf Makroviren gescannt. Diese Option ist nur verfügbar, wenn die Option **Standardmäßige und zusätzliche Dateitypen** aktiviert ist.

    HINWEIS
    Ein Scan auf Makroviren in allen Dateien könnte die Leistungsfähigkeit beeinträchtigen.
- **Angegebene Dateitypen**: Nur die von Ihnen angegebenen Dateitypen werden gescannt.
  - **Angegebene**: Klicken Sie bei Auswahl von **Angegebene Dateitypen** auf **Angegebene**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Die Liste der Dateityperweiterungen kann auch als Standardliste definiert werden. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen benutzerdefinierter Dateityperweiterungen* auf Seite 76.

    Der Zugriffsscanner kann maximal 1.000 angegebene Erweiterungen auflisten.

7 Klicken Sie unter **Nicht zu scannende Elemente** auf **Ausschlüsse**, um die Dateien, Ordner und Laufwerke anzugeben, die nicht gescannt werden sollen. Ausführliche Anweisungen dazu finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.

8 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

9 Wiederholen Sie Schritt 3 bis Schritt 8, um Erkennungseinstellungen für Vorgänge mit geringem oder hohem Risiko auszuwählen.

Hinzufügen von Dateityperweiterungen

Fügen Sie der Standardliste der Dateitypen benutzerdefinierte Dateitypen hinzu. Sie können die Funktion auch verwenden, um zuvor hinzugefügte benutzerspezifische Dateitypen wieder zu entfernen. Die Standardliste sowie alle vorhandenen benutzerdefinierten Dateitypen werden im Verlauf von Scan-Vorgängen geprüft.

> **HINWEIS**
> Sie können in der Standardliste der Dateitypen keine Dateitypen bearbeiten oder löschen. Die Standardliste wird von der zuletzt heruntergeladenen DAT-Datei definiert. Wenn Sie nicht möchten, dass bestimmte Erweiterungen gescannt werden, müssen Sie sie ausschließen. Weitere Informationen finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.

1 Klicken Sie auf **Ergänzungen**, um das Dialogfeld **Zusätzliche Dateitypen** zu öffnen.

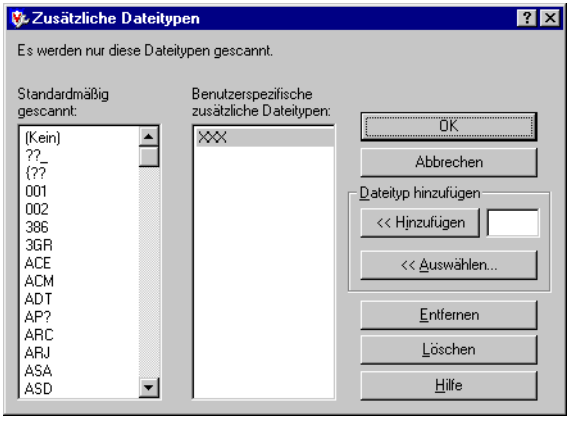


Abbildung 3-15. Zusätzliche Dateitypen

2 Sie können unter **Dateityp hinzufügen** benutzerdefinierte Dateityperweiterungen auf zwei verschiedene Arten hinzufügen:

- Geben Sie eine Dateityperweiterung in das Textfeld ein und klicken Sie auf **Hinzufügen**.

HINWEIS
Sie brauchen nur die ersten drei Buchstaben der Dateityperweiterung einzugeben. Wenn Sie die Dateinamenerweiterung HTM eingeben, sucht der Scanner nach Dateien des Typs HTM und HTML. Sie können Platzhalter oder eine Kombination aus Zeichen und Platzhaltern verwenden.

- Klicken Sie auf **Auswählen**, um das Dialogfeld **Dateityp auswählen** zu öffnen. Wählen Sie eine oder mehrere Dateityperweiterungen aus der Liste aus und klicken Sie auf **OK**.

  Mit der Tastenkombination STRG + UMSCHALTTASTE können Sie mehrere Dateityperweiterungen auswählen.

Die von Ihnen hinzugefügten Dateityperweiterungen werden in der Liste **Benutzerspezifische zusätzliche Dateitypen** angezeigt.

3 Sie können benutzerdefinierte Dateityperweiterungen aus der benutzerdefinierten Liste auf zwei Arten entfernen:

- Wählen Sie in der Liste **Benutzerspezifische zusätzliche Dateitypen** eine oder mehrere Dateityperweiterungen aus und klicken Sie auf **Entfernen**.
- Klicken Sie auf **Löschen**, um alle Elemente aus der Liste **Benutzerspezifische zusätzliche Dateitypen** zu entfernen.

Hinzufügen benutzerdefinierter Dateityperweiterungen

Erstellen Sie eine Liste von benutzerdefinierten Dateityperweiterungen, die im Verlauf von Scan-Operationen gescannt werden sollen. Sie können die Funktion auch verwenden, um zuvor hinzugefügte benutzerspezifische Dateitypen wieder zu entfernen.

1 Klicken Sie auf **Angegebene**, um das Dialogfeld **Angegebene Dateitypen** zu öffnen.



Abbildung 3-16. Angegebene Dateitypen

2 Sie können unter **Dateityp hinzufügen** benutzerdefinierte Dateityperweiterungen auf zwei verschiedene Arten hinzufügen:

- Geben Sie eine Dateityperweiterung in das Textfeld ein und klicken Sie auf **Hinzufügen**.

  HINWEIS
  Sie brauchen nur die ersten drei Buchstaben der Dateityperweiterung einzugeben. Wenn Sie die Dateinamenerweiterung HTM eingeben, sucht der Scanner nach Dateien des Typs HTM und HTML. Sie können Platzhalter oder eine Kombination aus Zeichen und Platzhaltern verwenden.

- Klicken Sie auf **Auswählen**, um das Dialogfeld **Dateityp auswählen** zu öffnen. Wählen Sie eine oder mehrere Dateityperweiterungen aus der Liste aus und klicken Sie auf **OK**.

Die von Ihnen hinzugefügten Dateityperweiterungen werden in der Liste unter **Es werden nur diese Dateitypen gescannt** angezeigt.

3 Sie können benutzerdefinierte Dateityperweiterungen auf zwei Arten aus der Liste entfernen:

- Wählen Sie in der Liste unter **Es werden nur diese Dateitypen gescannt** eine oder mehrere Dateityperweiterungen aus und klicken Sie auf **Entfernen**.

- Klicken Sie auf **Löschen**, um alle Elemente aus der Liste unter **Es werden nur diese Dateitypen gescannt** zu entfernen.

4 Klicken Sie auf **Auf Standard setzen**, um die aktuelle Liste benutzerdefinierter Dateityperweiterungen durch die Standardliste zu ersetzen. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zur Registerkarte **Erkennung** zurückzukehren.

Ausschließen von Dateien, Ordnern und Laufwerken

Geben Sie Dateien, Ordner und Laufwerke an, die von Scan-Vorgängen auszuschließen sind. Sie können die Funktion auch verwenden, um zuvor angegebene Ausschlüsse wieder zu entfernen.

1 Klicken Sie auf **Ausschlüsse**, um das Dialogfeld **Ausschlüsse festlegen** zu öffnen.

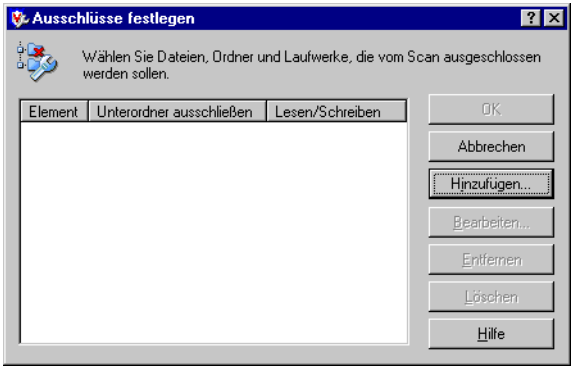


Abbildung 3-17. Ausschlüsse festlegen

2 Hinzufügen oder Bearbeiten von Dateien, Ordnern oder Laufwerken *Der Windows-Dateischutz wird standardmäßig aufgelistet.*

- Wenn Sie ein Element hinzufügen möchten, klicken Sie auf **Hinzufügen**, um das Dialogfeld **Ausschlusselement hinzufügen** zu öffnen.
- Wenn Sie ein Element bearbeiten möchten, doppelklicken Sie darauf oder wählen Sie es aus und klicken Sie auf **Bearbeiten**, um das Dialogfeld **Ausschlusselement bearbeiten** zu öffnen.

  HINWEIS
  Die Ausschlusseigenschaften sind stets dieselben, unabhängig davon, ob Sie ein Ausschlusselement hinzufügen oder bearbeiten.

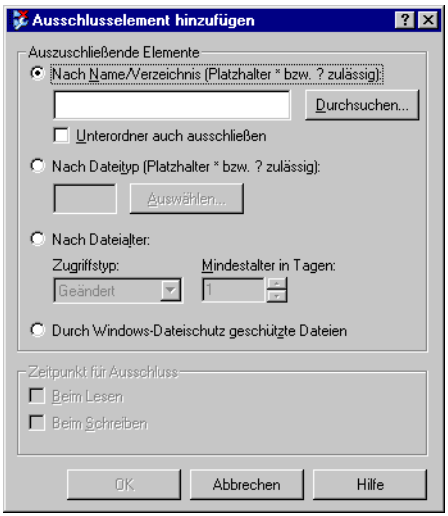


Abbildung 3-18. Ausschlusselement hinzufügen

3 Wählen Sie unter **Auszuschließende Elemente** eine der folgenden Optionen aus:

- **Nach Name/Verzeichnis**: *Diese Option ist standardmäßig ausgewählt*. Geben Sie den Namen oder das Verzeichnis an. Die Platzhalter * und ? sind zulässig. Sie können spezifische Informationen in das Textfeld eingeben oder auf **Durchsuchen** klicken, um einen Namen oder ein Verzeichnis zu suchen.

  HINWEIS
  Sie können vollständige Pfadangaben, z. B. C:\WINNIT\SYSTEM*, oder Dateinamen, z. B. PAGEFILE.SYS oder PAGEFILE.*, P*.* oder *.SYS, oder auch Ordnernamen, wie beispielsweise BACKUP, festlegen. Wenn Sie beispielsweise BACKUP angeben, werden alle Ordner mit der Bezeichnung BACKUP unabhängig von ihrem Speicherort ausgeschlossen.

Bei der Verwendung von Platzhaltern gelten folgende Einschränkungen:

- Gültige Platzhalter sind ? für den Ausschluss einzelner Zeichen und * für den Ausschluss mehrerer Zeichen.
- Ein \ kann nicht auf einen Platzhalter folgen. Beispielsweise ist C:\ABC\WWW? gültig, aber C:\ABC\WWW?\123 nicht.
- Ein Ausschluss, der nicht mit einem Pfad oder \ beginnt, wie WWW*, wird nur als Datei behandelt.
- Ein Ausschluss, der ?-Zeichen enthält, wird angewendet, wenn die Anzahl der Zeichen der Länge des Datei- oder Ordnernamens entspricht. Beispielsweise schließt der Ausschluss W?? WWW aus, aber nicht WW oder WWWW.
- **Unterordner auch ausschließen**: Wenn Sie die Option **Nach Name/Verzeichnis** ausgewählt haben, können Sie die Unterordner der Ordner ausschließen, die mit dem angegebenen Kriterium übereinstimmen.

- **Nach Dateityp**: Geben Sie eine Dateierweiterung nach Typ an. Geben Sie eine Dateierweiterung in das Textfeld ein oder klicken Sie auf **Auswählen**, um das Dialogfeld **Dateityp auswählen** zu öffnen, in dem Sie eine oder mehrere Erweiterungen aus der Liste auswählen können. Klicken Sie auf **OK**, um Ihre Einträge zu speichern und das Dialogfeld zu schließen.

  HINWEIS
  Die Dateierweiterung, die Sie angeben, kann Platzhalter enthalten. Gültige Platzhalter sind ? für den Ausschluss einzelner Zeichen und * für den Ausschluss mehrerer Zeichen.

- **Nach Dateialter**: Geben Sie an, ob Sie Dateien aufgrund ihres Alters ausschließen wollen.
  - **Zugriffstyp**: Wenn Sie die Option **Nach Dateialter** ausgewählt haben, klicken Sie auf , um den Zugriffstyp **Geändert** oder **Erstellt** auszuwählen.
  - **Mindestalter in Tagen**: Wenn Sie die Option **Nach Dateialter** ausgewählt haben, geben Sie das Mindestalter der Datei in Tagen an. Die Datei muss mindestens x Tage alt sein, bevor sie ausgeschlossen wird.

- **Durch Windows-Dateischutz geschützte Dateien**: Dieser Ausschluss basiert auf dem Windows-Dateischutzstatus einer Datei.

4 Geben Sie unter **Zeitpunkt für Ausschluss** an, wann die Elemente vom Scannen ausgeschlossen werden sollen:

- **Beim Lesen**: *Diese Option ist standardmäßig ausgewählt.* Die Ausschlusselemente werden beim Lesen von der Festplatte vom Scannen ausgeschlossen.
- **Beim Schreiben**: *Diese Option ist standardmäßig ausgewählt.* Die Ausschlusselemente werden beim Schreiben auf die Festplatte vom Scannen ausgeschlossen.

> **HINWEIS**
> Die Optionen **Beim Lesen** und **Beim Schreiben** stehen für Scan-Tasks auf Anforderung nicht zur Verfügung.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Ausschlüsse festlegen** zurückzukehren.

6 Sie können benutzerdefinierte Dateityperweiterungen auf zwei Arten aus der Liste entfernen:

- Wählen Sie in der Liste eine oder mehrere Dateityperweiterungen aus und klicken Sie auf **Entfernen**.
- Klicken Sie auf **Löschen**, um alle Elemente aus der Liste zu entfernen.

7 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zur Registerkarte **Erkennung** zurückzukehren.

8 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erweiterte Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erweitert**, um erweiterte Scan-Optionen für Heuristik, Nicht-Viren-Programmdateien und komprimierte Dateien festzulegen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.

2 Wählen Sie **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden** aus.

> **HINWEIS**
> Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

3 Wählen Sie **Vorgänge mit geringem Risiko** oder **Vorgänge mit hohem Risiko** aus.

4 Wählen Sie die Registerkarte **Erweitert** aus.

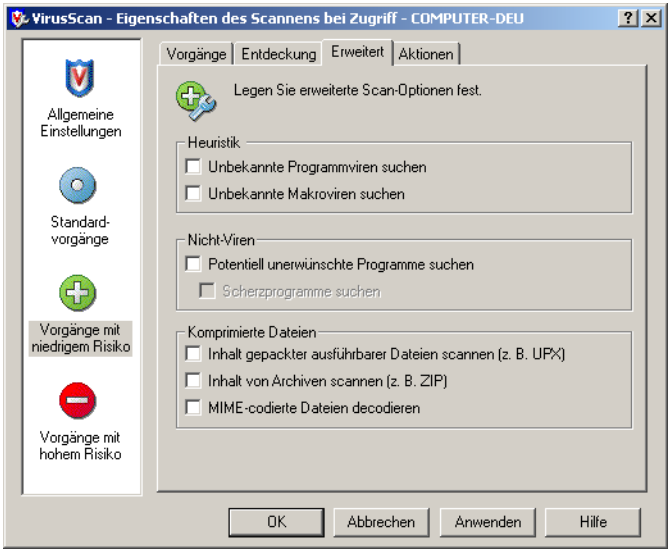


Abbildung 3-19. Vorgänge mit geringem oder hohem Risiko – Registerkarte "Erweitert"

HINWEIS

Nachdem Sie das Vorgangssymbol im linken Bereich ausgewählt haben, sind die weiteren Schritte zur Festlegung von Optionen für **Erweitert** für Vorgänge mit geringem oder hohem Risiko identisch.

5 Geben Sie unter **Heuristik** an, ob der Scanner die Wahrscheinlichkeit bewerten soll, mit der es sich bei unbekanntem Code oder Microsoft Office-Makros um Viren handelt. Wenn diese Funktion aktiviert ist, analysiert der Scanner, wie wahrscheinlich es ist, dass es sich bei dem Code um Varianten bekannter Viren handelt. Wählen Sie eine beliebige Kombination dieser Optionen:

- **Unbekannte Programmviren suchen**: *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt*. Ausführbare Dateien mit virenähnlichem Code werden wie infizierte Dateien behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion an.
- **Unbekannte Makroviren suchen**: *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt*. Eingebettete Makros mit virenähnlichem Code werden wie infizierte Makros behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

HINWEIS
Diese Option ist nicht mit der Option **Alle Dateien auch auf Makroviren scannen** auf der Registerkarte **Erkennung** identisch, mit der der Scanner nach allen bekannten Makroviren sucht. Mit dieser Option wird der Scanner angewiesen, die *Wahrscheinlichkeit* zu bewerten, mit der es sich bei einem unbekannten Makro um ein Virus handelt.

6 Geben Sie unter **Nicht-Viren** an, ob der Scanner nach potenziell unerwünschten Nicht-Viren-Anwendungen suchen soll.

- **Potenziell unerwünschte Programme suchen**: Potenziell unerwünschte Programme werden erkannt.
  - **Scherzviren suchen**: Wenn Sie die Option **Potenziell unerwünschte Programme suchen** gewählt haben, können Sie auch nach Scherzprogrammen suchen.

WARNUNG
VirusScan Enterprise unternimmt keine Maßnahmen gegen potenziell unerwünschte Programmdateien oder Scherzprogramme, die entdeckt werden. Erkennungen werden in der Protokolldatei protokolliert.

Wenn Sie bei einer erkannten, potenziell unerwünschten Programmdatei oder einem Scherzprogramm aktiv werden möchten, müssen Sie dies manuell tun. Wenn Sie z. B. ein erkanntes Scherzprogramm entfernen möchten, müssen Sie es manuell entfernen.

7 Wählen Sie unter **Komprimierte Dateien** aus, welche Typen von komprimierten Dateien vom Scanner überprüft werden sollen. Sie haben folgende Optionen:

- **Inhalt gepackter ausführbarer Dateien scannen**: *Diese Option ist für Standardvorgänge und Vorgänge mit hohem Risiko standardmäßig ausgewählt.* Komprimierte Dateien mit ausführbaren Programmdateien werden überprüft. Eine verpackte Programmdatei wird beim Ausführen niemals auf einen Datenträger, sondern immer direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.
- **Inhalt von Archiven scannen**: Archivdateien und ihr Inhalt werden überprüft. Eine Archivdatei ist eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann. Die in Archiven enthaltenen Dateien werden gescannt, bevor Sie auf Datenträgern gespeichert werden.
- **MIME-codierte Dateien decodieren**: Multipurpose Internet Mail Extensions-(MIME) kodierte Dateien werden erkannt, dekodiert und dann gescannt.

HINWEIS
Das Scannen komprimierter Dateien verbessert zwar den Schutz, dafür kann sich jedoch auch die für den Scan-Vorgang benötigte Zeit erhöhen.

8 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

9 Wiederholen Sie Schritt 3 bis Schritt 8, um erweiterte Einstellungen für Vorgänge mit geringem oder hohem Risiko auszuwählen.

Aktionseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Aktionen**, um die primären und sekundären Aktionen festzulegen, die beim Erkennen eines Virus vom Scan-Programm ausgeführt werden sollen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Zugriff** und wählen Sie anschließend im linken Bereich die Option **Alle Vorgänge**.

2 Wählen Sie **Unterschiedliche Einstellungen für Vorgänge mit geringem oder hohem Risiko verwenden** aus.

HINWEIS
Das Symbol **Alle Vorgänge** ändert sich in **Standardvorgänge** und sowohl die Symbole **Vorgänge mit geringem Risiko** als auch **Vorgänge mit hohem Risiko** werden im linken Fensterbereich verfügbar, wenn Sie diese Option auswählen.

3 Wählen Sie **Vorgänge mit geringem Risiko** oder **Vorgänge mit hohem Risiko** aus.

4 Wählen Sie die Registerkarte **Aktionen**.

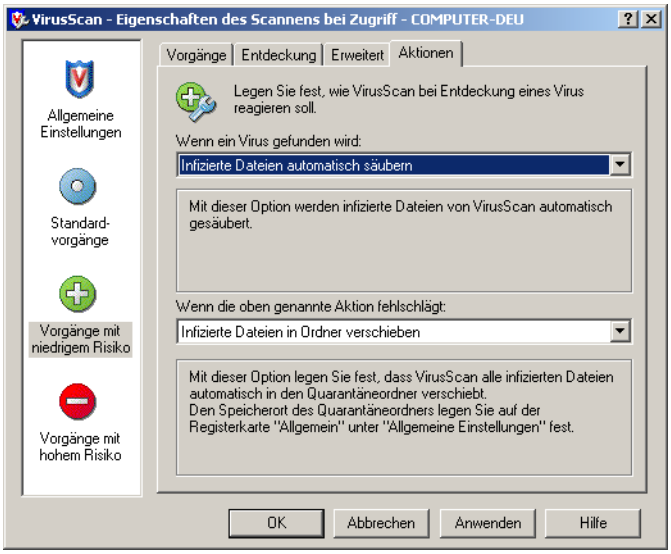

VirusScan - Eigenschaften des Scannens bei Zugriff - COMPUTER-DEU
Allgemeine Einstellungen
Standard-vorgänge
Vorgänge mit niedrigem Risiko
Vorgänge mit hohem Risiko
Vorgänge
Entdeckung
Erweitert
Aktionen
Legen Sie fest, wie VirusScan bei Entdeckung eines Virus reagieren soll.
Wenn ein Virus gefunden wird:
Infizierte Dateien automatisch säubern
Mit dieser Option werden infizierte Dateien von VirusScan automatisch gesäubert.
Wenn die oben genannte Aktion fehlschlägt:
Infizierte Dateien in Ordner verschieben
Mit dieser Option legen Sie fest, dass VirusScan alle infizierten Dateien automatisch in den Quarantäneordner verschiebt.
Den Speicherort des Quarantäneordners legen Sie auf der Registerkarte "Allgemein" unter "Allgemeine Einstellungen" fest.
OK
Abbrechen
Anwenden
Hilfe

Abbildung 3-20. Vorgänge mit geringem oder hohem Risiko – Registerkarte "Aktionen"

HINWEIS
Nachdem Sie das Vorgangssymbol im linken Bereich ausgewählt haben, sind die weiteren Schritte zur Festlegung von Optionen für die **Aktionen** für Vorgänge mit geringem oder hohem Risiko identisch.

5 Wählen Sie unter **Wenn ein Virus gefunden wird** die primäre Aktion aus, die das Scan-Programm ausführen soll, wenn ein Virus gefunden wird.

HINWEIS
Die primäre Standardaktion ist **Infizierte Dateien automatisch säubern**.

Klicken Sie auf ▼, um eine dieser Aktionen auszuwählen:

- **Zugriff auf infizierte Dateien verweigern** Allen Benutzern wird der Zugriff auf vom Scanner gefundene infizierte Dateien verweigert. Denken Sie daran, unter **Allgemeine Einstellungen** auf der Registerkarte **Berichte** die Eigenschaft **In Datei protokollieren** zu aktivieren, damit aufgezeichnet wird, welche Dateien infiziert sind.

HINWEIS
Wenn die Datei von einer externen Quelle, z. B. CD-ROM oder Internet, auf das lokale System geschrieben wird, fügt der Scanner am Ende des Dateinamens die Erweiterung .VIR hinzu. Der Scanner betrachtet diese Art der Dateiaktion als *Schreib*aktion.

Wenn die Datei z. B. von einem Speicherort auf der Festplatte an einen anderen Speicherort kopiert wird, wird die Erweiterung .VIR nicht dem Dateinamen hinzugefügt. Der Scanner betrachtet dies als *Verschiebe*aktion.

- **Infizierte Dateien in Ordner verschieben**: Der Scanner verschiebt infizierte Dateien in einen Ordner, der standardmäßig mit *quarantine* benannt ist. Sie können unter **Allgemeine Einstellungen** auf der Registerkarte **Allgemein** im Textfeld **Quarantäneordner** den Namen des Ordners ändern.

- **Infizierte Dateien automatisch löschen**: Der Scanner löscht infizierte Dateien sofort nach dem Entdecken. Denken Sie daran, unter **Allgemeine Einstellungen** auf der Registerkarte **Berichte** die Eigenschaft **In Datei protokollieren** zu aktivieren, damit aufgezeichnet wird, welche Dateien infiziert sind.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

  WARNUNG
  Wenn Sie auf der Registerkarte **Erweitert** die Option **Unbekannte Makroviren suchen** ausgewählt haben, wird die hier von Ihnen festgelegte Aktion auf alle Makros mit virenähnlichem Code angewendet. Bei Auswahl der Option **Infizierte Dateien automatisch löschen** werden alle Dateien mit Code, der Makroviren ähnelt, und alle Archive, die eine infizierte Datei enthalten, gelöscht. Wenn Sie das nicht beabsichtigen, sollten Sie sicherstellen, dass die von Ihnen getroffene Auswahl an Aktionen der für Makros getroffenen Auswahl an Aktionen entspricht.

- **Infizierte Dateien automatisch säubern**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner versucht, den Virus aus der infizierten Datei zu entfernen. Wenn der Scanner den Virus nicht entfernen kann oder der Virus die Datei irreparabel beschädigt hat, führt der Scanner die sekundäre Aktion aus. Weitere Informationen finden Sie unter Schritt 6.

6 Wählen Sie unter **Wenn die oben genannte Aktion fehlschlägt** die sekundäre Aktion aus, die das Scan-Programm beim Fehlschlagen der primären Aktion ausführen soll. Welche Optionen hierfür verfügbar sind, hängt von der Auswahl der primären Aktion ab.

HINWEIS
Bei der sekundären Standardaktion handelt es sich um **Infizierte Dateien in Ordner verschieben**.

Klicken Sie auf , um die sekundäre Aktion auszuwählen:

- **Zugriff auf infizierte Dateien verweigern**
- **Infizierte Dateien in Ordner verschieben**: *Diese Option ist standardmäßig ausgewählt.*
- **Infizierte Dateien automatisch löschen**

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

8 Wiederholen Sie Schritt 3 bis Schritt 7, um Aktionseinstellungen für Vorgänge mit geringem oder hohem Risiko auszuwählen.

Anzeigen von Scan-Ergebnissen

Sie können die Ergebnisse Ihrer Zugriffsscan-Operationen in der statistischen Übersicht sowie im Aktivitätsprotokoll anzeigen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Anzeigen von Scan-Statistiken
- Anzeigen des Aktivitätsprotokolls

Anzeigen von Scan-Statistiken

In der Zusammenfassung **Statistische Daten zum Scannen bei Zugriff** werden die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Rufen Sie mit einer der folgenden Methoden die Seiten **Statistische Daten zum Scannen bei Zugriff** auf:

- Doppelklicken Sie auf in der Systemablage.
- Klicken Sie mit der rechten Maustaste in der Taskliste auf den Zugriffsscan-Task und wählen Sie anschließend **Statistik**.

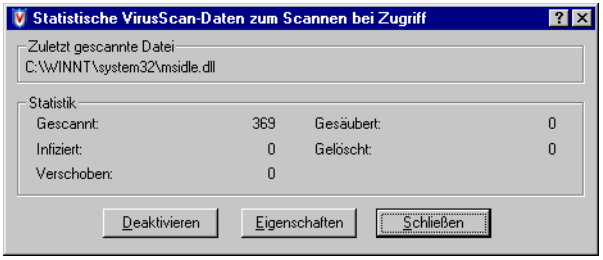


Abbildung 3-21. Statistische Daten zum Scannen bei Zugriff

Im Dialogfeld **Statistische VirusScan-Daten zum Scannen bei Zugriff** wird im oberen Bereich die **Zuletzt gescannte Datei** angezeigt, während der untere Bereich eine statistische Übersicht enthält.

3 Sie können eine dieser Funktionen ausführen, wenn Sie über Administratorrechte verfügen und gegebenenfalls das Kennwort eingeben.

> **HINWEIS**
> Die Schaltflächen **Deaktivieren** und **Eigenschaften** werden ausgeblendet, wenn die Benutzeroberfläche so konfiguriert ist, dass minimale Menüoptionen angezeigt werden. Diese Option können Sie unter **Extras** | **Benutzeroberflächenoptionen** | **Anzeigeoptionen** festlegen.

- Klicken Sie auf **Deaktivieren**, um den Zugriffsscanner zu deaktivieren. Mit dieser Funktion schalten Sie zwischen **Aktivieren** und **Deaktivieren** um.
- Klicken Sie auf **Eigenschaften**, um das Dialogfeld **Eigenschaften des Scannens bei Zugriff** zu öffnen, nehmen Sie an den entsprechenden Scan-Eigenschaften die gewünschten Änderungen vor und klicken Sie anschließend auf **Anwenden**, um die Änderungen zu übernehmen.

  Die von Ihnen festgelegten neuen Einstellungen für Scan-Vorgänge werden sofort wirksam.

4 Wenn Sie die Prüfung der Scan-Statistiken beendet haben, klicken Sie auf **Schließen**.

Anzeigen des Aktivitätsprotokolls

Das Aktivitätsprotokoll für das Scannen bei Zugriff zeigt spezifische Details zum ausgeführten Scan-Vorgang an. In der Zusammenfassung werden beispielsweise die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Öffnen Sie die Aktivitätsprotokolldatei mit einer der folgenden Methoden:

- Markieren Sie den Task und wählen Sie dann im Menü **Task** die Option **Aktivitätsprotokoll**.
- Klicken Sie mit der rechten Maustaste auf den Task in der Taskliste und wählen Sie die Option **Protokoll anzeigen**.

3 Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

Reaktionen auf die Erkennung von Viren

Der Zugriffsscanner sucht auf der Grundlage der von Ihnen im Dialogfeld **Eigenschaften des Scannens bei Zugriff** ausgewählten Konfigurationseinstellungen nach Viren. Weitere Informationen finden Sie unter *Konfigurieren des Zugriffsscanners* auf Seite 46. Bei der Erkennung von Viren werden diese Aktionen ausgeführt:

- Sie erhalten eine Benachrichtigung, wenn Sie den Warnungs-Manager und/oder den Zugriffsscanner so konfiguriert haben, dass bei der Erkennung eines Virus eine Nachricht an Sie gesendet werden soll.
- Der Zugriffsscanner zeichnet im Dialogfeld **Nachrichten vom Scannen bei Zugriff** eine Meldung auf.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Empfangen von Benachrichtigungen über die Erkennung von Viren
- Anzeigen der Nachrichten vom Zugriffsscanner
- Durchführen von Aktionen bei einer Viruserkennung

Empfangen von Benachrichtigungen über die Erkennung von Viren

Der Zugriffsscanner kann drei Arten von Benachrichtigungen senden, wenn er einen Virus findet:

- **Dialogfeld "Nachrichten vom Scannen bei Zugriff"**: Wenn Sie den Zugriffsscanner entsprechend konfiguriert haben, wird das Dialogfeld **Nachrichten vom Scannen bei Zugriff** bei der Erkennung eines Virus angezeigt. Weitere Informationen zum Konfigurieren der Benachrichtigungsoptionen finden Sie unter *Benachrichtigungseigenschaften* auf Seite 51.

  Ausführliche Informationen zum Dialogfeld **Nachrichten vom Scannen bei Zugriff** finden Sie unter *Anzeigen der Nachrichten vom Zugriffsscanner* auf Seite 91.

- **Messenger-Dienst für Netzwerk-Benutzer**: Wenn der Zugriffsscanner entsprechend konfiguriert wurde, erhalten Benutzer des Netzwerks bei der Virenerkennung eine entsprechende Meldung. Weitere Informationen zum Konfigurieren der Benachrichtigungsoptionen finden Sie unter *Benachrichtigungseigenschaften* auf Seite 51.

  Die Meldung enthält Details zur infizierten Datei, wie beispielsweise den Dateinamen und -speicherort, den Typ der erkannten Viren sowie die Version des Scan-Moduls und der DAT-Datei, die zur Erkennung des Virus verwendet wurde. Rufen Sie die Meldungsdetails auf und klicken Sie anschließend auf **OK**, um die Meldung zu schließen.

- **Messenger-Dienst**: Wenn Sie den Warnungs-Manager entsprechend konfiguriert haben, wird eine Netzwerkmeldung angezeigt. Weitere Informationen finden Sie unter *Konfigurieren des Warnungs-Managers* auf Seite 162.

  Nachstehend finden Sie ein Beispiel für eine vom Warnungs-Manager versendete Netzwerknachricht.

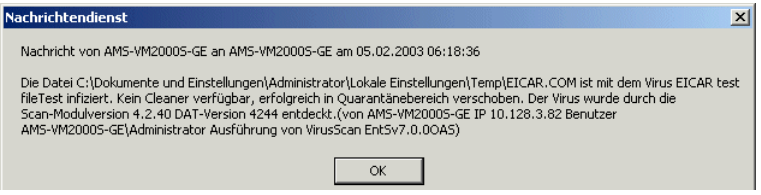

Nachrichtendienst
Nachricht von AMS-VM2000S-GE an AMS-VM2000S-GE am 05.02.2003 06:18:36
Die Datei C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temp\EICAR.COM ist mit dem Virus EICAR test fileTest infiziert. Kein Cleaner verfügbar, erfolgreich in Quarantänebereich verschoben. Der Virus wurde durch die Scan-Modulversion 4.2.40 DAT-Version 4244 entdeckt.(von AMS-VM2000S-GE IP 10.128.3.82 Benutzer AMS-VM2000S-GE\Administrator Ausführung von VirusScan Ent5v7.0.0OA5)
OK

Abbildung 3-22. Scannen bei Zugriff – Messenger-Dienst

Die Meldung enthält Details zur infizierten Datei, wie beispielsweise den Dateinamen und -speicherort, den Typ der erkannten Viren sowie die Version des Scan-Moduls und der DAT-Datei, die zur Erkennung des Virus verwendet wurde.

Je nachdem, wie Sie den Warnungs-Manager und den Zugriffsscanner konfiguriert haben, erhalten Sie möglicherweise mehrere Benachrichtigungen.

Rufen Sie die Meldungsdetails auf und klicken Sie anschließend auf **OK**, um die Meldung zu schließen.

HINWEIS
Wenn Sie nicht wenigstens eine der drei Optionen zum Versenden einer Nachricht beim Erkennen von Viren konfiguriert haben, erhalten Sie keine Benachrichtigungen. Sie können allerdings jederzeit das Dialogfeld **Nachrichten vom Scannen bei Zugriff** aufrufen, in dem erkannte Viren angezeigt werden. Weitere Informationen finden Sie unter *Anzeigen der Nachrichten vom Zugriffsscanner* auf Seite 91.

Anzeigen der Nachrichten vom Zugriffsscanner

Wenn Viren erkannt werden, zeichnet der Zugriffsscanner im Dialogfeld **Nachrichten vom Scannen bei Zugriff** eine Nachricht auf. In diesem Dialogfeld werden alle Nachrichten für den aktuellen Benutzer in chronologischer Reihenfolge angezeigt. Wenn es sich dabei um einen Benutzer mit Administratorrechten handelt, können darin optional alle auf dem lokalen System befindlichen Nachrichten angezeigt werden.

Dieses Dialogfeld wird beim Erkennen von Viren automatisch geöffnet, falls Sie den Zugriffsscanner entsprechend konfiguriert haben.

Sie können das Dialogfeld jederzeit öffnen, indem Sie mit der rechten Maustaste in der Systemablage auf  klicken und die Option **Nachrichten vom Scannen bei Zugriff** wählen.

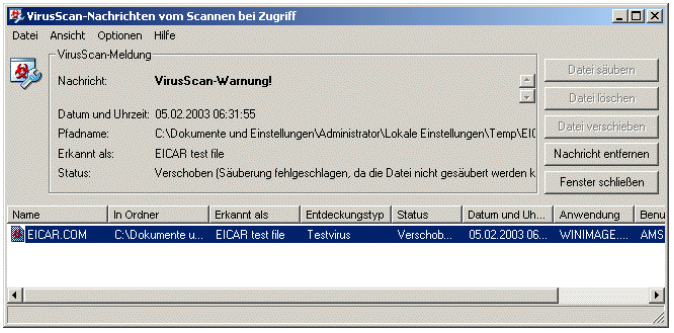


Abbildung 3-23. Nachrichten vom Scannen bei Zugriff

Das Dialogfeld **Nachrichten vom Scannen bei Zugriff** ist in verschiedene Bereiche unterteilt:

- **Menüs**: Bietet Menüs mit Optionen für Dateien und Nachrichten.
  - Im Menü **Datei** stehen Aktionen für in der Liste enthaltenen Dateien oder Nachrichten zur Auswahl.
  - Das Menü **Ansicht** enthält Optionen, mit denen Sie die Sichtbarkeit von Teilen des Dialogfelds steuern können.
  - Im Menü **Optionen** stehen Optionen zur Verfügung, mit denen Sie alle Nachrichten anzeigen bzw. festlegen können, dass das Dialogfeld **Nachrichten vom Scannen bei Zugriff** immer im Vordergrund angezeigt wird.

- Das Menü **Hilfe** bietet Zugriff auf Hilfethemen zum VirusScan Enterprise-Produkt, Zugriff auf Virusinformationen, eine Option zur Übermittlung von Beispielen und Zugriff auf Websites für technischen Support sowie auf Informationen zum aktuell installierten Produkt und der entsprechenden Lizenz, zum Scan-Modul und den DAT-Dateien.

- **VirusScan-Nachricht**: Zeigt spezifische Daten zur ausgewählten Nachricht an.
- **Schaltflächen**: Schaltflächen für Aktionen, die für die ausgewählte Nachricht ausgewählt werden können. Wenn eine Aktion für die ausgewählte Nachricht nicht verfügbar ist, wird die entsprechende Schaltfläche deaktiviert.
- **Nachrichtenliste**: Listet die Nachrichten zu Viren auf, die vom Zugriffsscanner erkannt wurden. Die Spalten der Liste können durch Klicken auf die Spaltenüberschrift sortiert werden.
- **Statusleiste**: Zeigt den Status der ausgewählten Nachricht an.

Durchführen von Aktionen bei einer Viruserkennung

Dieser Abschnitt beschreibt die Aktionen, die Sie durchführen können, wenn der Zugriffsscanner einen Virus erkennt.

> **HINWEIS**
> Sie haben außerdem die Möglichkeit, ein Virusbeispiel zur Analyse an AVERT zu senden. Weitere Informationen finden Sie unter *Einsenden eines Virenbeispiels* auf Seite 41.

Verwenden Sie das Dialogfeld **Nachrichten vom Zugriffsscanner**, um bei der Erkennung von Viren durch den Zugriffsscanner geeignete Aktionen auszuführen.

1. Klicken Sie in der Systemablage mit der rechten Maustaste auf  und wählen Sie anschließend die Option **Nachrichten vom Scannen bei Zugriff**.
2. Markieren Sie eine Meldung in der Liste und wählen Sie dann eine Aktion mit einer der folgenden Methoden:

   - Menü **Datei.**
   - Schaltflächen für die Auswahl einer Aktion.
   - Klicken Sie mit der rechten Maustaste auf die hervorgehobene Nachricht und wählen Sie die Aktion aus.

   Nachstehend finden Sie eine Auflistung der Aktionen, die Sie in der Liste auswählen können:

   Datei säubern: Versucht, die in der gewählten Meldung angegebene Datei zu säubern.

In bestimmten Fällen können Dateien nicht gesäubert werden. Dies wird dadurch bedingt, dass entweder keine entsprechenden Bereinigungsfunktionen verfügbar sind oder der Virus die Datei irreparabel geschädigt hat. Wenn die Datei nicht gesäubert werden kann, fügt der Scanner dem Dateinamen die Erweiterung VIR hinzu und verweigert den Zugriff darauf. In der Protokolldatei wird ein entsprechender Eintrag erfasst.

HINWEIS
Wenn eine Datei nicht gesäubert werden kann, wird empfohlen, die Datei zu löschen und anschließend aus einem nicht infizierten Sicherungsverzeichnis wiederherzustellen.

Datei verschieben: Verschiebt die in der gewählten Meldung angegebenen Dateien in den Quarantäneordner. Der Speicherort des Quarantäneordners wird im Dialogfeld **Eigenschaften des Scannens bei Zugriff** auf der Registerkarte **Allgemein** unter **Allgemeine Einstellungen** festgelegt.

Datei löschen: Löscht die in der gewählten Meldung angegebene Datei. Der Dateiname wird im Protokoll aufgezeichnet, so dass Sie die Datei aus einer Sicherungskopie wiederherstellen können.

Alles auswählen (STRG+A): In der Liste werden alle Nachrichten ausgewählt.

Nachricht entfernen (STRG+D): Entfernt die gewählte Meldung aus der Liste. Nachrichten, die aus der Liste entfernt wurden, werden in der Protokolldatei weiterhin angezeigt.

Wenn eine Aktion für die aktuelle Nachricht nicht verfügbar ist, werden das entsprechende Symbol, die Schaltfläche und die Menüeinträge deaktiviert. Die Option **Datei säubern** ist beispielsweise nicht verfügbar, wenn die Datei bereits gelöscht wurde.

Mithilfe der Optionen auf der Registerkarte **Nachrichten**, die sich unter **Allgemeine Einstellungen** im Dialogfeld **Eigenschaften des Scannens bei Zugriff** befindet, können Administratoren festlegen, welche Aktionen Benutzer ohne Administratorrechte an Nachrichten in der Liste vornehmen können. Wenn eine Aktion vom Administrator unterdrückt wird, wird die Schaltfläche ausgeblendet und das entsprechende Symbol sowie die Menüeinträge deaktiviert.

Folgende weitere Aktionen stehen zur Verfügung:

- **Protokolldatei öffnen**: Öffnet die Datei mit dem Aktivitätsprotokoll.
- **Fenster schließen**: Schließt das Dialogfeld **Nachrichten vom Scannen bei Zugriff**.

Scannen auf Anforderung 4

Mit dem Anforderungsscanner verfügen Sie über eine Methode, mit der Sie alle Teile des Computers zu für Sie günstigen Zeiten oder in regelmäßigen Abständen auf Viren scannen können. Verwenden Sie ihn als Ergänzung zum kontinuierlichen Schutz durch den Zugriffsscanner oder um regelmäßige Scan-Vorgänge so festzulegen, dass Ihre Arbeitsabläufe nicht eingeschränkt werden.

Vorgangsscans im Speicher und inkrementelles Scannen machen die Virenerkennung effizienter denn je.

- Bei Vorgangsscans im Speicher werden alle aktiven Vorgänge überprüft, bevor das Scannen auf Anforderung durchgeführt wird. Wenn infizierte Vorgänge gefunden werden, wird die Infektion markiert und der Vorgang angehalten. Das bedeutet, dass nur ein einziger Durchlauf mit dem Anforderungsscanner erforderlich ist, um alle Vorkommnisse eines Virus zu entfernen.
- Inkrementelle oder fortsetzbare Scan-Vorgänge ermöglichen dem Scanner, dort weiterzumachen, wo der Scan zuletzt unterbrochen wurde. Sie können einen Anfangs- und Endzeitpunkt für geplante Scans festlegen. Der Anforderungsscanner arbeitet sich in logischer Weise durch alle Ordner und zugehörigen Dateien. Wenn die Zeitbegrenzung erreicht ist, wird der Scan-Vorgang angehalten. Wenn beim nächsten geplanten Scan inkrementelles Scannen verwendet wird, wird der Anforderungs-Scan an der Stelle in der Datei- und Ordnerstruktur fortgesetzt, an der der vorhergehende Scan-Vorgang unterbrochen wurde.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Erstellen von Anforderungstasks
- Konfigurieren von Anforderungstasks
- Zurücksetzen oder Speichern von Standardeinstellungen
- Planen von Anforderungstasks
- Scan-Vorgänge
- Anzeigen von Scan-Ergebnissen
- Reaktionen auf die Erkennung von Viren

Erstellen von Anforderungstasks

Sie können Anforderungstasks mit drei verschiedenen Methoden erstellen. Der Scan-Typ, der erstellt wird (gespeichert oder nicht gespeichert), hängt von der verwendeten Methode ab. Wählen Sie eine der folgenden Optionen aus:

- Über das Menü **Start**– Aus dem Menü **Start** erstellte Tasks werden nicht gespeichert und sind für die einmalige Anwendung bestimmt, sofern Sie die Tasks nicht für eine spätere Verwendung speichern.
- Mithilfe des Symbols  in der Systemablage – Über die Systemablage erstellte Tasks werden nicht gespeichert und sind für die einmalige Verwendung bestimmt, sofern Sie die Tasks nicht für eine spätere Verwendung speichern.
- Mithilfe der **VirusScan-Konsole** – Über die Konsole erstellte Tasks werden in der Taskliste für eine spätere Verwendung gespeichert.

  HINWEIS
  Wenn Sie Aufforderungsscan-Tasks über ePolicy Orchestrator 3.0 oder höher erstellen und Tasksichtbarkeit aktivieren, sind diese Aufforderungsscan-Tasks in der VirusScan-Konsole sichtbar. Auf diese ePolicy Orchestrator-Tasks besteht nur *Lesezugriff* und sie können nicht von der VirusScan-Konsole aus konfiguriert werden. Weitere Informationen finden Sie im *VirusScan Enterprise Konfigurationshandbuch für die Verwendung mit ePolicy Orchestrator 3.0*.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Erstellen von Tasks mithilfe des Menüs "Start" oder der Systemablage
- Erstellen von Tasks über die Konsole

Erstellen von Tasks mithilfe des Menüs "Start" oder der Systemablage

Anforderungsscan-Tasks, die entweder mithilfe des Start-Menüs oder der Systemablage erstellt werden, sind für die einmalige Verwendung bestimmt und werden nicht gespeichert. Der erstellte Task kann dann konfiguriert, geplant und ausgeführt werden. Er wird jedoch beim Schließen des Dialogfelds **Scannen auf Anforderung – Eigenschaften** stets entfernt, wenn er nicht gespeichert wird.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Öffnen Sie **Scannen auf Anforderung – Eigenschaften** mithilfe einer der folgenden Methoden:

- Klicken Sie auf **Start** und wählen Sie anschließend **Programme** | **Network Associates** | **VirusScan-Anforderungsscan**.
- Klicken Sie in der Systemablage mit der rechten Maustaste auf  und wählen Sie anschließend die Option **Scannen auf Anforderung**.

Das Dialogfeld **Scannen auf Anforderung – Eigenschaften (nicht gespeicherter Task)** wird aufgerufen.

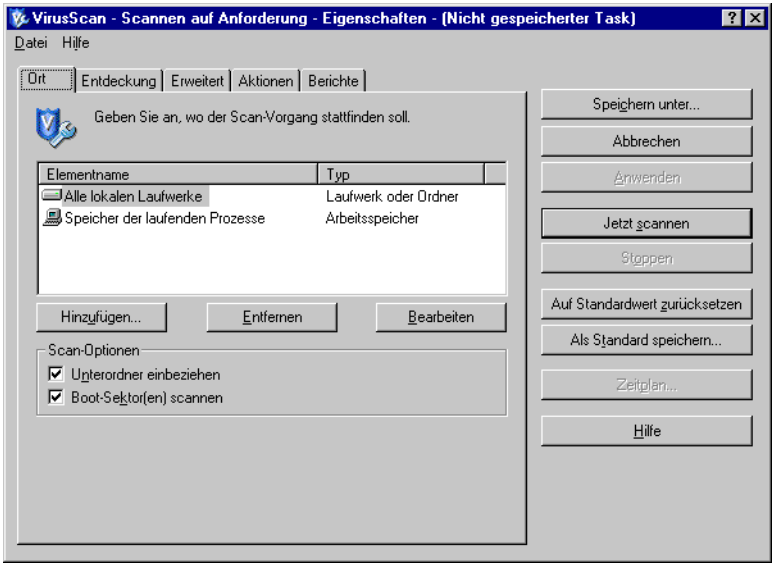


Abbildung 4-1. Scannen auf Anforderung – Eigenschaften (nicht gespeicherter Task)

HINWEIS
Anhand des Zusatzes **(nicht gespeicherter Task)** in der Titelleiste können Sie erkennen, dass es sich um einen Anforderungsscan-Vorgang handelt, der nicht gespeichert wird. Klicken Sie auf **Speichern unter**, um den Task in der Konsole für erneute Verwendung zu speichern. Nachdem Sie den Task gespeichert haben, wird in der Titelleiste des Dialogfelds **Scannen auf Anforderung – Eigenschaften** anstelle von **(nicht gespeicherter Task)** der angegebene Task-Name angezeigt.

3 Konfigurieren Sie einen Scan-Task auf Anforderung für den einmaligen Gebrauch, der nicht gespeichert wird. Ausführliche Anweisungen dazu finden Sie unter *Konfigurieren von Anforderungstasks* auf Seite 99.

4 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

5 Um den Task zu planen, müssen Sie ihn zuerst speichern und dann auf **Zeitplan** klicken. Ein nicht gespeicherter Task lässt sich nicht planen. Ausführliche Anweisungen dazu finden Sie unter *Task-Pläne konfigurieren* auf Seite 236.

6 Klicken Sie auf **Jetzt scannen**, um den Task auszuführen. Weitere Informationen finden Sie unter *Ausführen von Anforderungstasks* auf Seite 117.

Erstellen von Tasks über die Konsole

Die **VirusScan-Konsole** enthält einen Standard-Task für das Scannen auf Anforderung mit dem Namen **Alle stationären Datenträger**. Sie können diesen Task umbenennen und/oder eine unbegrenzte Anzahl von Anforderungstasks erstellen.

So erstellen Sie einen neuen Anforderungstask über die Konsole:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

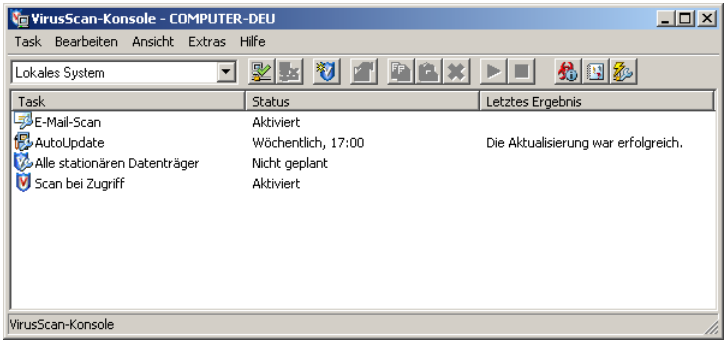


Abbildung 4-2. VirusScan-Konsole

2 Erstellen Sie einen neuen Scan-Task mithilfe einer der folgenden Methoden:

- Klicken Sie mit der rechten Maustaste in einen leeren Bereich der Konsole, *ohne ein Element in der Taskliste zu markieren*. Wählen Sie dann **Neuer Scan-Task**.
- Wählen Sie aus dem Menü **Task** die Option **Neuer Scan-Task**.
- Klicken Sie in der Symbolleiste der Konsole auf  .

In der Taskliste der **VirusScan-Konsole** wird ein neuer Anforderungstask markiert angezeigt.

3 Geben Sie für den Task einen neuen Namen ein und drücken Sie dann die EINGABETASTE, um das Dialogfeld **Scannen auf Anforderung – Eigenschaften** aufzurufen.

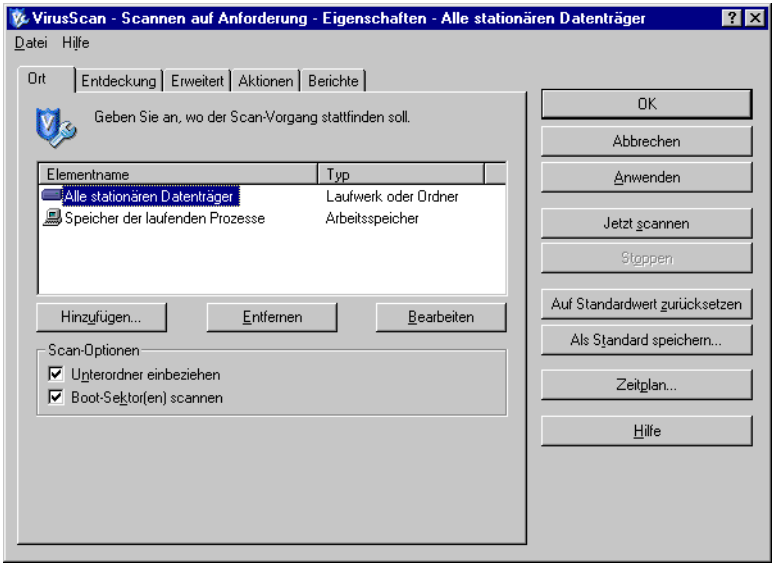


Abbildung 4-3. Scannen auf Anforderung – Eigenschaften

Konfigurieren von Anforderungstasks

Sie können beim Konfigurieren des Anforderungsscanners festlegen, welche Elemente zu welchem Zeitpunkt gescannt werden, welche Reaktion erfolgt, wenn Viren gefunden werden, und wie Sie in so einem Fall benachrichtigt werden sollen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Ortseigenschaften
- Erkennungseigenschaften
- Erweiterte Eigenschaften
- Aktionseigenschaften
- Berichtseigenschaften
- Hinzufügen von Elementen
- Entfernen von Elementen
- Bearbeiten von Elementen

Ortseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Ort**, um die Verzeichnisse festzulegen, die Sie nach Viren durchsuchen möchten.

1 Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.

2 Wählen Sie die Registerkarte **Ort** aus.

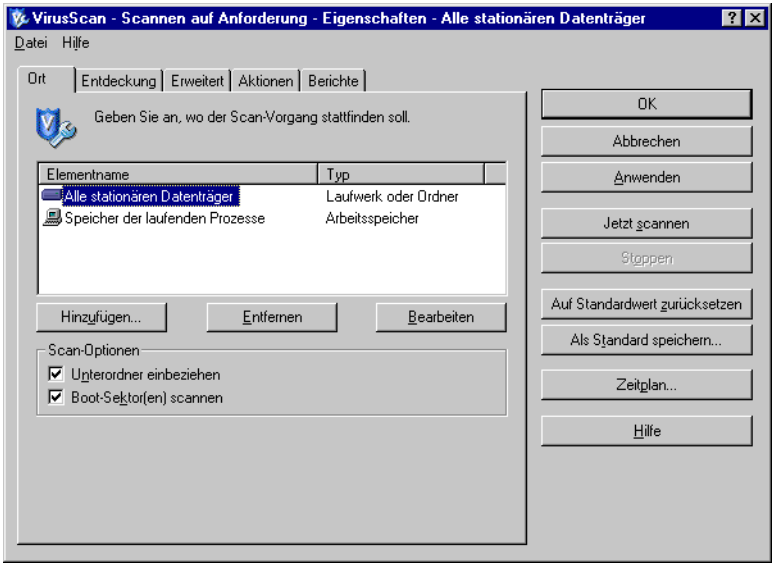


Abbildung 4-4. Scannen auf Anforderung – Eigenschaften: Registerkarte "Ort"

HINWEIS
Im Dialogfeld werden standardmäßig alle Laufwerke des Computers und alle darin enthaltenen Unterordner aufgelistet. Ein so umfassender Scan-Vorgang kann sehr viel Zeit beanspruchen. Beschränken Sie daher den Scan-Vorgang, wenn Sie ihn zukünftig regelmäßig ausführen möchten.

3 Geben Sie unter **Elementname** an, wo der Scan-Vorgang ausgeführt werden soll. Standardmäßig werden *alle stationären Laufwerke* und *Speicherkapazitäten der laufenden Vorgänge* aufgeführt.

HINWEIS
Wenn Sie eine neue Scan-Task erstellen, werden *alle lokalen Laufwerke* und *Speicherkapazitäten der laufenden Vorgänge* aufgeführt.

Verwenden Sie die Schaltflächen **Hinzufügen**, **Entfernen** und/oder **Bearbeiten**, um die zu scannenden Elemente festzulegen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen, Entfernen und Bearbeiten von Elementen* auf Seite 101.

4 Geben Sie unter **Scan-Optionen** zusätzliche Scan-Kriterien an. Wählen Sie eine der folgenden Optionen aus:

- **Unterordner einbeziehen**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner überprüft alle Unterordner in den zum Scannen ausgewählten Volumes. Wenn die ausgewählten Datenträger nur auf der Stammebene gescannt werden sollen, deaktivieren Sie das Kontrollkästchen **Unterordner einbeziehen**.
- **Boot-Sektor(en) scannen** *Diese Option ist standardmäßig ausgewählt.* Der Scanner überprüft den Boot-Sektor der Festplatte. In einigen Fällen kann es angebracht sein, die Analyse des Boot-Sektors zu deaktivieren, z. B. wenn eine Festplatte einen speziellen oder anormalen Boot-Sektor besitzt, der keinem Viren-Scan unterzogen werden kann.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Hinzufügen, Entfernen und Bearbeiten von Elementen

Führen Sie die folgenden Schritte aus, wenn Sie der Liste **Elementname** im Dialogfeld **Scannen auf Anforderung – Eigenschaften**Elemente**hinzufügen**, daraus **entfernen** oder **bearbeiten** möchten.

- Hinzufügen von Elementen
- Entfernen von Elementen
- Bearbeiten von Elementen

Hinzufügen von Elementen

1 Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.

2 Klicken Sie auf der Registerkarte **Ort** auf **Hinzufügen**, um das Dialogfeld **Scan-Element hinzufügen** zu öffnen.

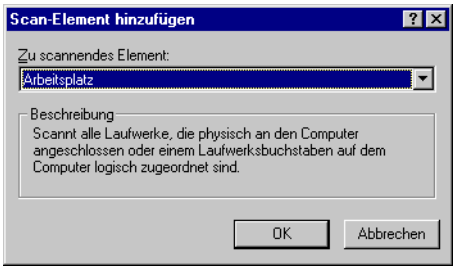


Abbildung 4-5. Scan-Element hinzufügen

3 Klicken Sie auf , um ein Scan-Element aus der Liste auszuwählen. Wählen Sie eine der folgenden Optionen aus:

- **Arbeitsplatz**: *Diese Option ist standardmäßig ausgewählt.* Alle lokalen und zugeordneten Laufwerke werden gescannt.
- **Alle lokalen Laufwerke**: Alle Laufwerke des Computers sowie alle darin enthaltenen Unterordner werden gescannt.
- **Alle stationären Datenträger**: Alle physisch mit dem Computer verbundenen Festplatten werden gescannt.
- **Alle Wechseldatenträger**: Ausschließlich Disketten, CD-ROMs, ZIP-Disketten von Iomega oder ähnliche Speichermedien, die physisch mit dem Computer verbunden sind, werden gescannt.
- **Alle Netzlaufwerke**: Scannt Netzlaufwerke, die einem Laufwerksbuchstaben auf dem Computer logisch zugeordnet sind.
- **Speicher der laufenden Prozesse**: Der Speicher aller aktuell ausgeführten Prozesse wird gescannt. Dieser Scan-Vorgang wird vor allen weiteren Scan-Vorgängen ausgeführt.
- **Stammordner des Benutzers**: Der Stammordner des Benutzers, der den Scan-Vorgang startet, wird gescannt.
- **Profilordner des Benutzers**: Das Profil des Benutzers, der den Scan-Vorgang startet, wird gescannt. Dazu gehört auch der Ordner "Eigene Dateien".
- **Laufwerk oder Ordner**: Ein bestimmtes Laufwerk oder ein bestimmter Ordner wird gescannt. Geben Sie in das Textfeld **Speicherort** den Pfad zu dem Laufwerk oder Ordner ein oder klicken Sie auf **Durchsuchen**, um das Laufwerk oder den Ordner zu suchen und auszuwählen.

  Wenn Sie diesen Schritt beendet haben, klicken Sie auf **OK**, um zum Dialogfeld **Scan-Element hinzufügen** zurückzukehren.
- **Datei**: Eine bestimmte Datei wird gescannt. Geben Sie in das Textfeld **Speicherort** den Pfad zu der Datei ein oder klicken Sie auf **Durchsuchen**, um das Dialogfeld **Zu scannendes Element auswählen** zu öffnen, in dem Sie eine Datei suchen und auswählen können.

  Wenn Sie ein Element ausgewählt haben, klicken Sie auf **Öffnen**, um zum Dialogfeld **Scan-Element hinzufügen** zurückzukehren.

4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Scannen auf Anforderung – Eigenschaften** zurückzukehren.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Entfernen von Elementen

1. Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.
2. Wählen Sie auf der Registerkarte **Ort** in der Liste **Elementname** ein oder mehrere zu löschende Elemente aus und klicken Sie auf **Entfernen**.
3. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie das Element entfernen möchten.
4. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Bearbeiten von Elementen

1. Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.
2. Wählen Sie auf der Registerkarte **Ort** in der Liste **Elementname** ein Element aus und klicken Sie auf **Bearbeiten**, um das Dialogfeld **Scan-Element bearbeiten** zu öffnen.

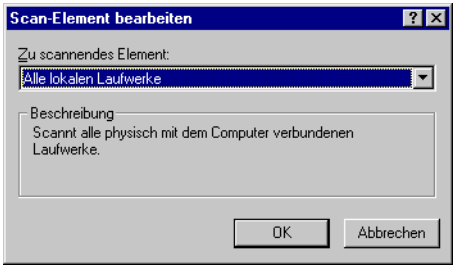


Abbildung 4-6. Scan-Element bearbeiten

3. Klicken Sie auf , um ein Scan-Element aus der Liste **Zu scannendes Element** auszuwählen. *Alle lokalen Laufwerke sind standardmäßig ausgewählt.*

   HINWEIS
   Die hier verfügbaren Optionen sind dieselben wie beim **Hinzufügen von Elementen**. Eine vollständige Liste sowie eine Beschreibung der Optionen finden Sie unter Schritt 3 auf Seite 102.

4. Klicken Sie auf **OK**, um zum Dialogfeld **Scannen auf Anforderung – Eigenschaften** zurückzukehren.
5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erkennungseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erkennung**, um festzulegen, welche Dateitypen beim Scannen auf Anforderung zu welchem Zeitpunkt überprüft werden.

1. Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.
2. Wählen Sie die Registerkarte **Erkennung**.

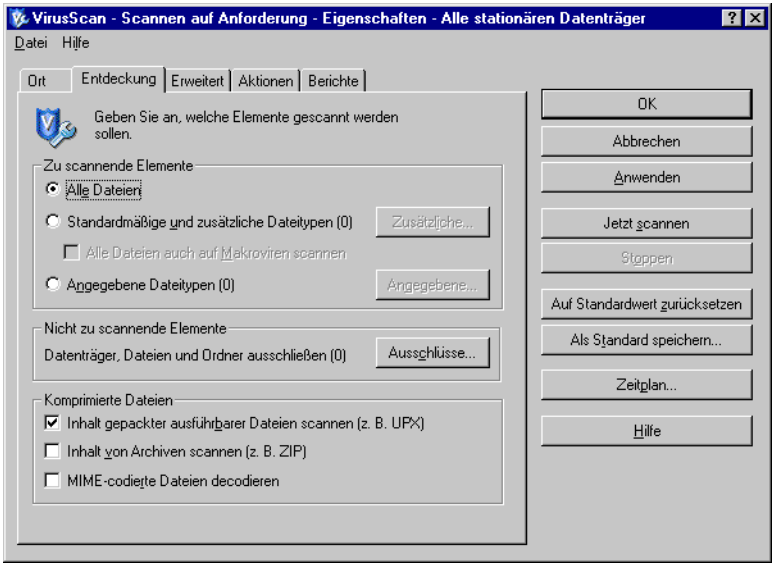


Abbildung 4-7. Scannen auf Anforderung – Eigenschaften: Registerkarte "Erkennung"

3 Wählen Sie unter **Zu scannende Elemente** eine der folgenden Optionen:

- **Alle Dateien**: *Diese Option ist standardmäßig ausgewählt.* Alle Dateien (unabhängig von der Erweiterung) werden gescannt.
- **Standardmäßige und zusätzliche Dateitypen**: Die standardmäßig aufgelisteten Erweiterungen und alle zusätzlich angegebenen Dateitypen werden gescannt. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert. Sie können benutzerdefinierte Dateityperweiterungen hinzufügen und entfernen, aber keine Dateityperweiterungen aus der Standardliste löschen. Sie können in der Standardliste vorhandene Erweiterungen auch ausschließen. Weitere Informationen finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.
  - **Ergänzungen**: Klicken Sie bei Auswahl von **Standardmäßige und zusätzliche Dateitypen** auf **Ergänzungen**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen von Dateityperweiterungen* auf Seite 75.

    Die Liste des Anforderungsscanners kann maximal 1.000 zusätzliche Erweiterungen umfassen.
  - **Alle Dateien auch auf Makroviren scannen**: Alle Dateien werden unabhängig von der Erweiterung auf Makroviren gescannt. Diese Option ist nur verfügbar, wenn die Option **Standardmäßige und zusätzliche Dateitypen** aktiviert ist.

    HINWEIS
    Ein Scan auf Makroviren in allen Dateien könnte die Leistungsfähigkeit beeinträchtigen.
- **Angegebene Dateitypen**: Nur die von Ihnen angegebenen Dateitypen werden gescannt.
  - **Angegebene**: Klicken Sie bei Auswahl von **Angegebene Dateitypen** auf **Angegebene**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Die Liste der Dateityperweiterungen kann auch als Standardliste definiert werden. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen benutzerdefinierter Dateityperweiterungen* auf Seite 76.

    Die Liste des Anforderungsscanners kann maximal 1.000 angegebene Erweiterungen umfassen.

4 Klicken Sie unter **Nicht zu scannende Elemente** auf **Ausschlüsse**, um die Dateien, Ordner und Laufwerke anzugeben, die nicht gescannt werden sollen. Ausführliche Anweisungen dazu finden Sie unter *Ausschließen von Dateien, Ordnern und Laufwerken* auf Seite 78.

5 Wählen Sie unter **Komprimierte Dateien** aus, welche Typen von komprimierten Dateien vom Scanner überprüft werden sollen. Sie haben folgende Optionen:

- **Inhalt gepackter ausführbarer Dateien scannen**: *Diese Option ist standardmäßig ausgewählt.* Komprimierte Dateien mit ausführbaren Programmdateien werden überprüft. Eine verpackte Programmdatei wird beim Ausführen niemals auf einen Datenträger, sondern immer direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.
- **Inhalt von Archiven scannen**: Archivdateien und ihr Inhalt werden überprüft. Eine Archivdatei ist eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann. Die in Archiven enthaltenen Dateien werden gescannt, bevor Sie auf Datenträgern gespeichert werden.
- **MIME-codierte Dateien decodieren**: Multipurpose Internet Mail Extensions-(MIME) kodierte Dateien werden erkannt, dekodiert und dann gescannt.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erweiterte Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erweitert**, um erweiterte Scan-Eigenschaften, z. B. Scannen nach unbekannten Programmviren und potenziell unerwünschten Programmen, den Anteil der CPU-Auslastung und sonstige Optionen festzulegen.

1 Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.

2 Wählen Sie die Registerkarte **Erweitert** aus.

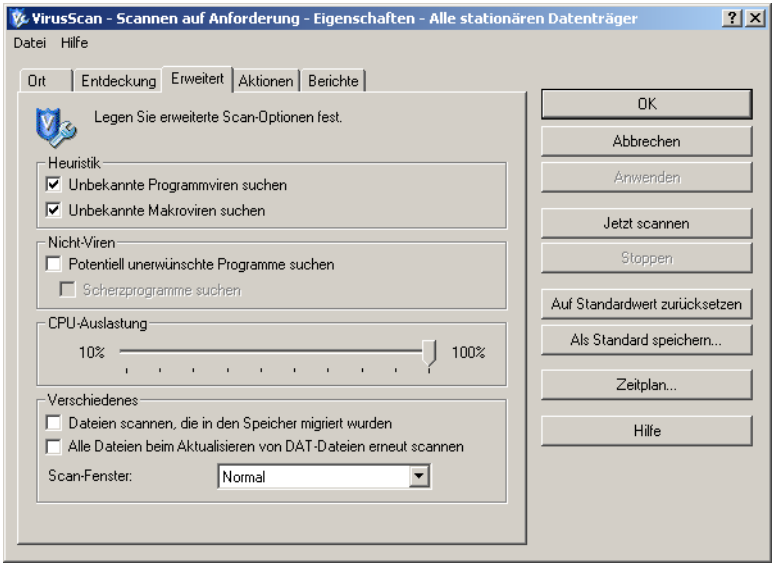


Abbildung 4-8. Scannen auf Anforderung – Eigenschaften: Registerkarte "Erweitert"

3 Geben Sie unter **Heuristik** an, ob der Scanner die Wahrscheinlichkeit bewerten soll, mit der es sich bei unbekanntem Code oder Microsoft Office-Makros um Viren handelt. Wenn diese Funktion aktiviert ist, analysiert der Scanner, wie wahrscheinlich es ist, dass es sich hierbei um Varianten bekannter Viren handelt. Wählen Sie eine beliebige Kombination dieser Optionen:

- **Unbekannte Programmviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Ausführbare Dateien mit virenähnlichem Code werden wie infizierte Dateien behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion an.
- **Unbekannte Makroviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Eingebettete Makros mit virenähnlichem Code werden wie infizierte Makros behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

  HINWEIS
  Diese Option ist nicht mit der Option **Alle Dateien auch auf Makroviren scannen** auf der Registerkarte **Erkennung** identisch, mit der der Scanner nach allen bekannten Makroviren sucht. Mit dieser Option wird der Scanner angewiesen, die *Wahrscheinlichkeit* zu bewerten, mit der es sich bei einem unbekannten Makro um ein Virus handelt.

4 Geben Sie unter **Nicht-Viren** an, ob der Scanner nach potenziell unerwünschten Nicht-Viren-Anwendungen suchen soll.

- **Potenziell unerwünschte Programme suchen**: Potenziell unerwünschte Programme werden erkannt.

  - **Scherzviren suchen**: Wenn Sie die Option **Potenziell unerwünschte Programme suchen** gewählt haben, können Sie auch nach potenziell unerwünschten Scherzprogrammen suchen.

    WARNUNG
    VirusScan Enterprise unternimmt keine Maßnahmen gegen potenziell unerwünschte Programmdateien oder Scherzprogramme, die entdeckt werden. Erkennungen werden in der Protokolldatei protokolliert.

    Wenn Sie bei einer erkannten potenziell unerwünschten Programmdatei oder einem Scherzprogramm aktiv werden möchten, müssen Sie dies manuell tun. Wenn Sie z. B. ein erkanntes Scherzprogramm entfernen möchten, müssen Sie es manuell entfernen.

5. Verwenden Sie den Regler unter **CPU-Auslastung**, um den Anteil der CPU-Auslastung für den Scan-Task im Verhältnis zu anderen auf dem Computer ausgeführten Tasks festzulegen. *Standardmäßig sind 100 % ausgewählt.* Dadurch wird sichergestellt, dass andere Software-Anwendungen während eines Scan-Vorgangs nicht langsamer ausgeführt werden. Der Scan-Vorgang dauert dadurch jedoch länger. Wenn der Scan-Task zu einem Zeitpunkt ausgeführt werden soll, zu dem die CPU durch andere wichtige Vorgänge stark beansprucht ist, sollten Sie den Anteil der CPU-Auslastung für den Scan-Task beschränken.

   HINWEIS
   Die Beschränkung der CPU-Auslastung zeigt beim Scannen von verschlüsselten Dateien keine Wirkung. Die Entschlüsselung erfolgt nicht durch den SCAN32-Vorgang, sondern durch den LSASS.EXE-Vorgang. Das Scannen von verschlüsselten Dateien lastet die CPU stark aus. Selbst bei einem niedrigen CPU-Auslastungsgrad auf dem Scan-Thread werden die Dateien mit einer ausreichend hohen Geschwindigkeit gescannt, so dass LSASS.EXE ausgelastet ist, um die entschlüsselten Daten bereitzustellen.

6. Wählen Sie unter **Verschiedenes** eine dieser Optionen:

   - **Dateien scannen, die in den Speicher migriert wurden**: Dateien, die in den Offline-Speicher migriert wurden, werden gescannt.

     HINWEIS
     Wenn Sie Remotespeicher verwenden, um den Speicherplatz auf dem Server zu erweitern, kann der Anforderungsscanner die zwischengespeicherten Dateien scannen.

Die Datenspeicherung in einem Remotespeicher erfolgt hierarchisch mithilfe von zwei definierten Ebenen. Die obere Ebene, der so genannte lokale Speicher, umfasst die NTFS-Datenträger des Computers, auf dem der Remotespeicher unter Windows 2000 Server ausgeführt wird. Die untere Ebene, der so genannte Remotespeicher, befindet sich in der automatischen Bandbibliothek oder auf dem eigenständigen Bandlaufwerk, das mit dem Server-Computer verbunden ist.

Durch die Remotespeicherung werden geeignete Dateien auf den lokalen Datenträgern automatisch in eine Bandbibliothek kopiert und der auf den lokalen Datenträgern verfügbare Speicherplatz wird überwacht. Dateidaten werden lokal zwischengespeichert, sodass ein schneller Zugriff bei Bedarf möglich ist. Falls erforderlich werden bei der Remotespeicherung Daten aus dem lokalen Speicher in den Remotespeicher verschoben. Wenn Sie auf eine Datei auf einem Datenträger zugreifen müssen, der vom Remotespeicher verwaltet wird, können Sie die Datei wie gewohnt öffnen. Wenn die Dateidaten nicht mehr auf dem lokalen Datenträger gespeichert sind, ruft der Remotespeicher die Daten aus einer Bandbibliothek ab.

- **Alle Dateien beim Aktualisieren von DAT-Dateien erneut scannen**: Beim Installieren oder Aktualisieren der neuen DAT-Dateien werden alle Dateien erneut gescannt. Das ist besonders für terminierte und wiederaufnehmbare Scan-Vorgänge hilfreich. Wenn Sie diese Funktion verwenden, minimieren Sie das Risiko einer Infektion durch eine erneute Überprüfung der Dateien auf neue Viren.
- **Scan-Fenster**: *Standardmäßig ist "Normal" ausgewählt.* Klicken Sie auf  , um festzulegen, wie das Scan-Fenster bei Anforderungsscans angezeigt werden soll. Folgende Optionen stehen zur Auswahl:
  - **Normal**
  - **Als Symbol**
  - **Verborgen**

  HINWEIS
  Das Scan-Fenster kann zwar so konfiguriert werden, dass es normal, als Symbol oder verborgen angezeigt wird, die Fenster für geplante Tasks und Remote-Tasks bleiben jedoch unabhängig von der Konfiguration immer verborgen.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Aktionseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Aktionen**, um die primären und sekundären Aktionen festzulegen, die beim Erkennen eines Virus vom Scan-Programm ausgeführt werden sollen.

1 Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.

2 Wählen Sie die Registerkarte **Aktionen**.

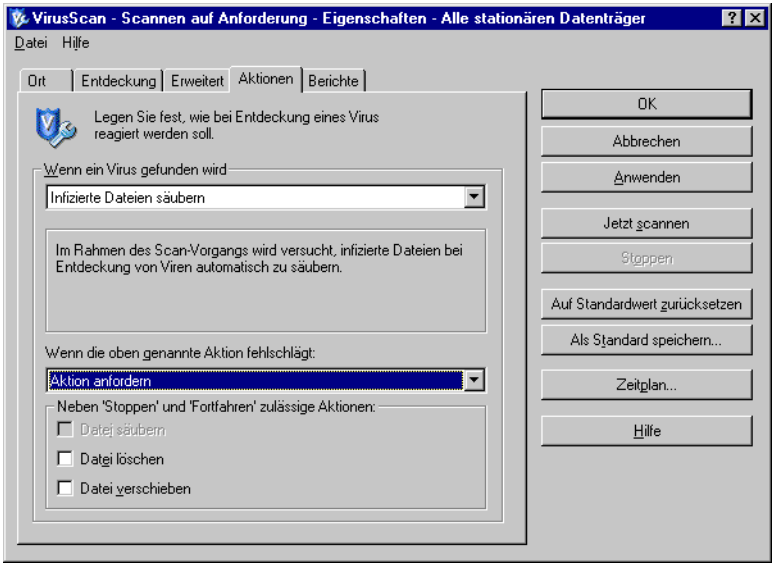


Abbildung 4-9. Scannen auf Anforderung – Eigenschaften: Registerkarte "Aktionen"

3 Wählen Sie unter **Wenn ein Virus gefunden wird** die primäre Aktion aus, die das Scan-Programm ausführen soll, wenn ein Virus gefunden wird.

> **HINWEIS**
> Die primäre Standardaktion ist **Infizierte Dateien säubern**.

Klicken Sie auf ▼, um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Bei Erkennung eines Virus wird eine Eingabeaufforderung an den Benutzer ausgegeben.

- Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben **Stoppen** und **Fortfahren** noch zulässig sind. Folgende Optionen stehen zur Auswahl:

  - **Datei säubern**: Die infizierte Datei kann gesäubert werden.
  - **Datei löschen**: Die infizierte Datei kann gelöscht werden.
  - **Datei verschieben**: Die infizierte Datei kann verschoben werden.

  Für diese Option ist keine sekundäre Aktion zulässig.

- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung einer infizierten Datei fortgesetzt.

  Für diese Option ist keine sekundäre Aktion zulässig.

  Infizierte Dateien in Ordner verschieben: Der Scanner verschiebt infizierte Dateien in einen *Quarantäne*ordner. Dabei können Sie den standardmäßigen Speicherort des Ordners im Textfeld **Ordner** übernehmen oder auf **Durchsuchen** klicken, um zum Speicherort des gewünschten Ordners zu wechseln.

  Der Standardspeicherort und der Name des Quarantäneordners lautet:

  ```
  <Laufwerk>:\quarantine
  ```

  HINWEIS
  Der Ordner *Quarantäneordner* darf nicht auf einer Diskette oder einem CD-Laufwerk, sondern muss auf der Festplatte gespeichert werden.

- **Infizierte Dateien säubern**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner versucht, den Virus aus der infizierten Datei zu entfernen. Wenn der Scanner den Virus nicht entfernen kann oder der Virus die Datei irreparabel beschädigt hat, führt der Scanner die sekundäre Aktion aus. Weitere Informationen finden Sie unter Schritt 4.

- **Infizierte Dateien löschen**: Der Scanner löscht infizierte Dateien sofort nach dem Entdecken. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Dateien in einem Bericht erfasst werden.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

WARNUNG
Wenn Sie auf der Registerkarte **Erweitert** die Option **Unbekannte Makroviren suchen** ausgewählt haben, wird die hier von Ihnen festgelegte Aktion auf alle Makros mit virenähnlichem Code angewendet. Bei Auswahl der Option **Infizierte Dateien löschen** werden alle Dateien mit Code, der Makroviren ähnelt, und alle Archive, die eine infizierte Datei enthalten, gelöscht. Wenn Sie das nicht beabsichtigen, sollten Sie sicherstellen, dass die von Ihnen getroffene Auswahl an Aktionen der für Makros getroffenen Auswahl an Aktionen entspricht.

4 Wählen Sie unter **Wenn die oben genannte Aktion fehlschlägt** die sekundäre Aktion aus, die das Scan-Programm beim Fehlschlagen der primären Aktion ausführen soll.

HINWEIS
Bei der sekundären Standardaktion handelt es sich um **Infizierte Dateien in Ordner verschieben**.

Klicken Sie auf , um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben **Stoppen** und **Fortfahren** noch zulässig sind. Folgende Optionen stehen zur Auswahl:
  - **Datei säubern**: Die infizierte Datei kann gesäubert werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Datei säubern** ausgewählt haben.
  - **Datei löschen**: Die infizierte Datei kann gelöscht werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Datei löschen** ausgewählt haben.
  - **Datei verschieben**: Die infizierte Datei kann verschoben werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Datei verschieben** ausgewählt haben.
- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung einer infizierten Datei fortgesetzt.
- **Infizierte Dateien in Ordner verschieben**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner verschiebt infizierte Dateien in einen *Quarantäne*ordner. Dabei können Sie den standardmäßigen Speicherort des Ordners im Textfeld **Ordner** übernehmen oder auf **Durchsuchen** klicken, um zum Speicherort des gewünschten Ordners zu wechseln.

  Der Standardspeicherort und der Name des Quarantäneordners lautet:

  ```
  <Laufwerk>:\quarantine
  ```

HINWEIS
Der Ordner *Quarantäneordner* darf nicht auf einer Diskette oder einem CD-Laufwerk, sondern muss auf der Festplatte gespeichert werden.

- **Infizierte Dateien löschen**: Der Scanner löscht infizierte Dateien sofort nach dem Entdecken. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Dateien in einem Bericht erfasst werden.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Berichtseigenschaften

Klicken Sie auf die Registerkarte **Berichte**, um die Protokollierungsaktivitäten zu konfigurieren. Geben Sie den Speicherort und die Größe der Protokolldatei sowie die Informationen an, die Sie pro Protokolleintrag erfassen möchten.

HINWEIS
Die Protokolldatei ist ein wichtiges Verwaltungstool, mit dem Sie Virenaktivitäten im Netzwerk verfolgen und die vom Scanner zur Erkennung und Behandlung erkannter Viren verwendeten Einstellungen festhalten können. Anhand der in der Datei protokollierten Ereignisse können Sie feststellen, welche Dateien durch Sicherungskopien ersetzt, im Quarantäneordner geprüft oder vom Rechner gelöscht werden müssen. Weitere Informationen finden Sie unter *Anzeigen des Aktivitätsprotokolls* auf Seite 121.

1 Öffnen Sie das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.

2 Wählen Sie die Registerkarte **Berichte**.

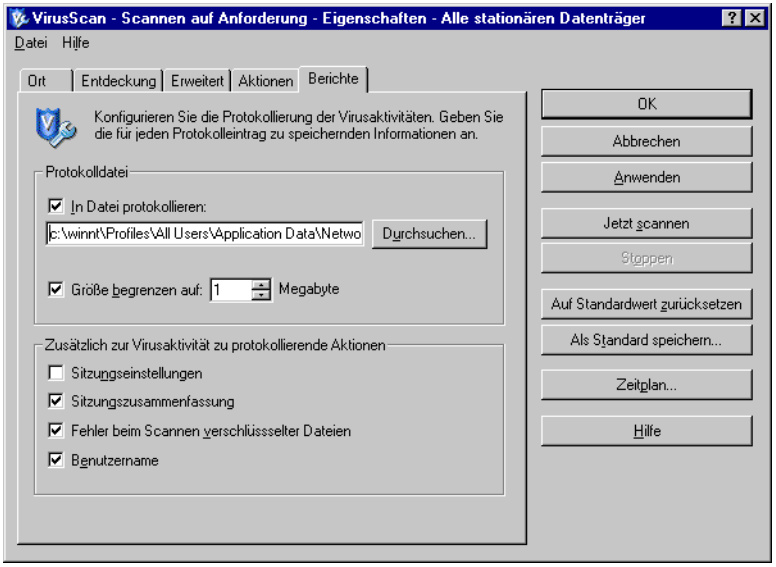


Abbildung 4-10. Scannen auf Anforderung – Eigenschaften: Registerkarte "Berichte"

3 Wählen Sie unter **Protokolldatei** eine dieser Optionen:

- **In Datei protokollieren**: *Diese Option ist standardmäßig ausgewählt.* Virusaktivitäten werden beim Scannen auf Anforderung in einer Protokolldatei aufgezeichnet.
- Sie können den im Textfeld angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einer anderen geeigneten Datei auf dem Computer oder im Netzwerk zu wechseln.

  HINWEIS
  Standardmäßig schreibt der Scanner Protokollinformationen in die Datei ONDEMANDSCANLOG.TXT in diesem Ordner:

  ```
  <Laufwerk>:Winnt\Profiles\All Users\Application
  Data\Network Associates\VirusScan
  ```

- **Größe begrenzen auf**: *Diese Option ist standardmäßig ausgewählt. Die Standardgröße der Protokolldatei ist 1 MB.* Übernehmen Sie die Standardgröße, oder legen Sie einen anderen Wert für die Protokolldatei fest. Wenn Sie diese Option auswählen, geben Sie einen Wert zwischen 1 MB und 999 MB ein.

HINWEIS
Wenn die Datenmenge in der Protokolldatei die von Ihnen festgelegte Dateigröße übersteigt, werden 20 Prozent der Protokolldateieinträge (die ältesten) gelöscht und der Datei neue Daten hinzugefügt.

4 Legen Sie unter **Zusätzlich zur Virusaktivität zu protokollierende Aktionen** fest, welche zusätzlichen Informationen in der Protokolldatei aufgezeichnet werden sollen:

- **Sitzungseinstellungen**: In der Protokolldatei werden die für die einzelnen Scan-Sitzungen ausgewählten Eigenschaften erfasst.
- **Sitzungszusammenfassung** *Diese Option ist standardmäßig ausgewählt.* Die Aktionen des Scanners bei den einzelnen Scan-Sitzungen werden zusammengefasst und der Protokolldatei hinzugefügt. Zu den Zusammenfassungsinformationen gehören die Anzahl der gescannten Dateien, Anzahl und Typ der entdeckten Viren, die Anzahl der verschobenen, gelöschten oder bereinigten Dateien sowie weitere Informationen.
- **Fehler beim Scannen verschlüsselter Dateien** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden die Namen der verschlüsselten Dateien erfasst, die nicht gescannt werden konnten.
- **Benutzername** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei wird der Name des Benutzers erfasst, der zum Zeitpunkt der Aufzeichnung der jeweiligen Protokolleinträge auf dem Computer angemeldet war.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Zurücksetzen oder Speichern von Standardeinstellungen

Nach dem Konfigurieren des Anforderungstasks können Sie die Konfigurationseinstellungen auf die Standardeinstellungen zurücksetzen oder die aktuelle Konfiguration als Standard speichern.

Wenn Sie weder die Standardeinstellungen wiederherstellen noch die aktuellen Einstellungen als Standard speichern möchten, lassen Sie diese Schritte aus.

1 Wählen Sie eine der folgenden Optionen aus:

- **Auf Standardwert zurücksetzen**: Die standardmäßigen Scan-Einstellungen werden wiederhergestellt.
- **Als Standard speichern**: Die aktuelle Scan-Konfiguration wird als Standardkonfiguration gespeichert. Bei Auswahl von **Als Standard speichern** werden alle neuen Tasks mit dieser Konfiguration gespeichert.

2 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Planen von Anforderungstasks

Nachdem ein Anforderungstask konfiguriert wurde, kann er so geplant werden, dass er an bestimmten Tagen, zu bestimmten Zeiten oder in bestimmten Abständen ausgeführt wird.

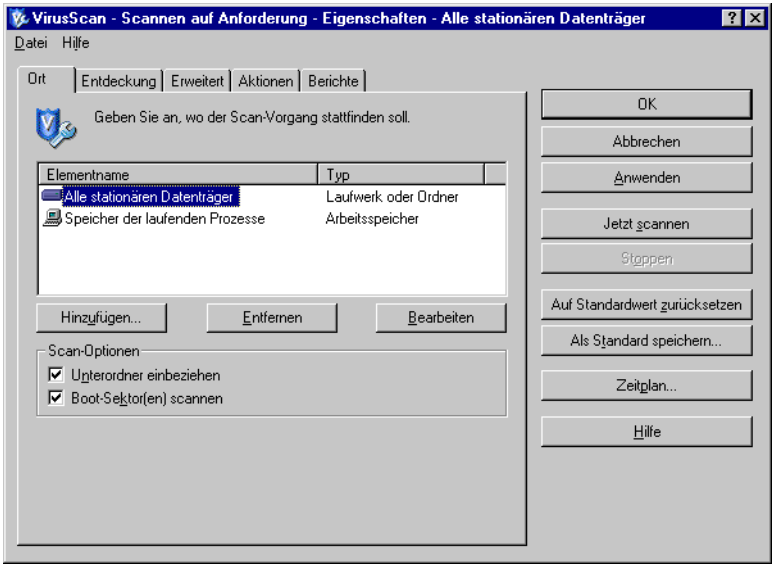


Abbildung 4-11. Scannen auf Anforderung – Eigenschaften: Zeitplan

1. Öffnen Sie für den zu konfigurierenden Task das Dialogfeld **Scannen auf Anforderung – Eigenschaften**.
2. Klicken Sie auf **Zeitplan**. Genaue Anweisungen zur Planung eines Tasks finden Sie unter *Planen von Tasks* auf Seite 235.

Scan-Vorgänge

Sie können geplante Anforderungstasks unbeaufsichtigt ausführen, Scan-Tasks sofort starten und sie während eines Scan-Vorgangs unterbrechen, beenden und neu starten.

HINWEIS
Der Anforderungsscanner scannt bei den Scan-Vorgängen nicht den eigenen *Quarantäneordner*. Er wurde so konzipiert, dass der *Quarantäneordner* bei den Scan-Vorgängen ausgelassen wird, um wiederholtes Scannen oder Scan-Schleifen zu vermeiden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Ausführen von Anforderungstasks
- Unterbrechen und Neustarten von Anforderungstasks
- Ausführen von Anforderungstasks
- Fortsetzbare Scan-Vorgänge

Ausführen von Anforderungstasks

Nachdem Sie den Task mit den gewünschten Scan-Eigenschaften konfiguriert haben, können Sie den Scan-Task mithilfe einer der folgenden Methoden ausführen:

- **Nach Zeitplan scannen**: Wenn der Scan-Vorgang zeitlich geplant wurde, können Sie den Task unbeaufsichtigt ausführen lassen.

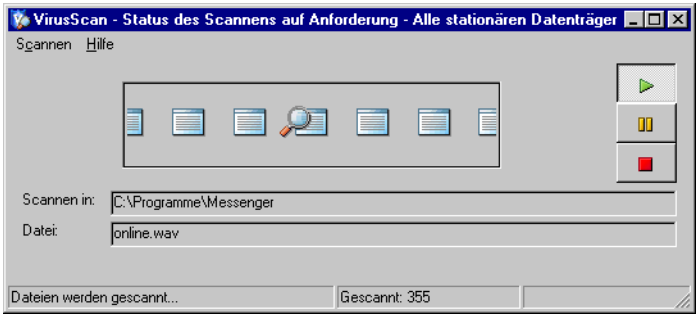


Abbildung 4-12. Scannen auf Anforderung – Scan-Vorgang läuft

HINWEIS
Damit der Scanner den Task ausführen kann, muss der Computer eingeschaltet sein. Wenn der Computer zum Zeitpunkt der geplanten Ausführung des Tasks heruntergefahren ist, wird der Task entweder zum nächsten geplanten Zeitpunkt gestartet, zu dem der Computer eingeschaltet ist, oder wenn der Computer neu gestartet wird. Hierfür muss jedoch auf der Registerkarte **Zeitplan** unter **Zeitplaneinstellungen** die Option **Ausgelassenen Task ausführen** aktiviert sein.

HINWEIS
Der Scanner wird nach der Ausführung der vom Planer gestarteten geplanten Tasks und der auf einem Remote-Computer ausgeführten Remote-Tasks immer beendet.

- **Sofortiges Scannen**: Sie können Anforderungsscan-Tasks sofort starten. Dazu stehen Ihnen mehrere Methoden zur Verfügung:
  - Erstellen Sie in der Systemablage oder im Start-Menü einen Scan-Task auf Anforderung, klicken Sie dann im Dialogfeld **Scannen auf Anforderung – Eigenschaften** auf **Jetzt scannen**.
  - Klicken Sie mit der rechten Maustaste in der **VirusScan-Konsole** auf einen Anforderungsscan-Task und wählen Sie **Starten**.
  - Klicken Sie in Windows-Explorer mit der rechten Maustaste auf eine Datei, einen Ordner, ein Laufwerk oder ein anderes Element und wählen Sie dann **Nach Viren scannen**.

    Das Dialogfeld **Scannen auf Anforderung** wird angezeigt.

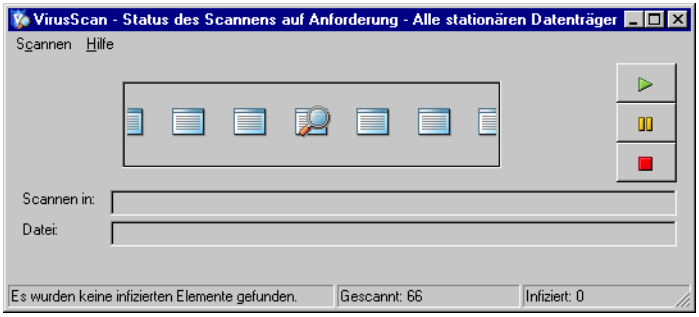


Abbildung 4-13. Scannen auf Anforderung – Scan-Vorgang läuft

HINWEIS
Der Scanner wird nach Ausführung dieser sofortigen Scan-Tasks nicht automatisch beendet. Wählen Sie zum Beenden des Scanners aus dem Menü **Scannen** die Option **Beenden**.

Unterbrechen und Neustarten von Anforderungstasks

Sie können Anforderungstasks beim Scan-Vorgang unterbrechen und neu starten.

- Klicken Sie zum Unterbrechen eines Anforderungstasks im Dialogfeld **Scannen auf Anforderung** auf .
- Klicken Sie zum Neustarten eines Anforderungstasks im Dialogfeld **Scannen auf Anforderung** auf .

Ausführen von Anforderungstasks

Sie können Anforderungstasks beim Scan-Vorgang mithilfe einer der folgenden Methoden beenden:

- Klicken Sie im Dialogfeld **Scannen auf Anforderung** auf .
- Klicken Sie im Dialogfeld **Scannen auf Anforderung – Eigenschaften** auf **Stoppen**.

Fortsetzbare Scan-Vorgänge

Der Anforderungsscanner setzt den Scan-Vorgang automatisch an der Stelle fort, an der er unterbrochen wurde, wenn der Scan-Vorgang vor Abschluss unterbrochen wurde. Die inkrementelle Scan-Funktion des Anforderungsscanners erkennt die zuletzt gescannte Datei. Beim nächsten Starten des Scanners können Sie entscheiden, den Scan-Vorgang an der unterbrochenen Stelle fortzusetzen oder von vorn zu beginnen.

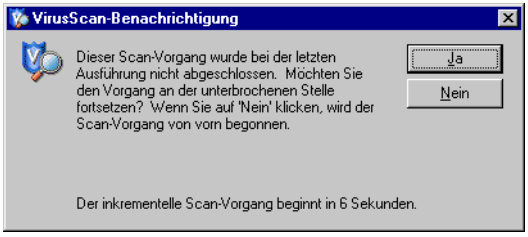

VirusScan-Benachrichtigung
Dieser Scan-Vorgang wurde bei der letzten Ausführung nicht abgeschlossen. Möchten Sie den Vorgang an der unterbrochenen Stelle fortsetzen? Wenn Sie auf 'Nein' klicken, wird der Scan-Vorgang von vorn begonnen.
Ja
Nein
Der inkrementelle Scan-Vorgang beginnt in 6 Sekunden.

Abbildung 4-14. Fortsetzbarer Scan-Vorgang

Anzeigen von Scan-Ergebnissen

Sie können die Ergebnisse Ihrer Anforderungsscan-Operationen in der statistischen Übersicht sowie im Aktivitätsprotokoll anzeigen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Anzeigen von Scan-Statistiken
- Anzeigen des Aktivitätsprotokolls

Anzeigen von Scan-Statistiken

In der Zusammenfassung **Statistische Daten zum Scannen auf Anforderung** werden die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

So zeigen Sie Statistiken und Ergebnisse für den Task an:

1 Klicken Sie mit der rechten Maustaste in der **VirusScan-Konsole** auf den Anforderungsscan-Task in der Taskliste und wählen Sie **Statistik**.

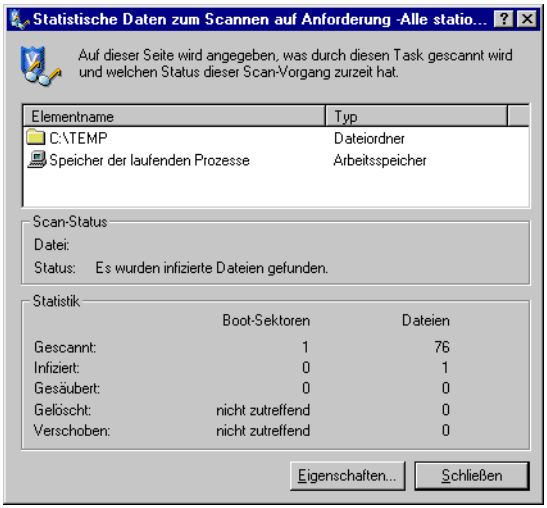


Abbildung 4-15. Statistische Daten zum Scannen auf Anforderung

Im oberen Bereich des Dialogfelds **Statistische Daten zum Scannen auf Anforderung** werden die für den Task gewählten Scan-Ziele angezeigt. Im mittleren Bereich wird der Status des Scan-Vorgangs angezeigt und der untere Bereich enthält eine statistische Zusammenfassung.

Wenn der Scan-Task noch nicht abgeschlossen ist, werden die aktuell überprüfte Datei sowie der Status des Scan-Vorgangs im mittleren Bereich angezeigt.

HINWEIS
Wenn der Task erneut ausgeführt wird, gelten die hier angezeigten Statistikdaten nur für den letzten Scan-Vorgang.

2 Klicken Sie auf **Eigenschaften**, um das Dialogfeld **Scannen auf Anforderung – Eigenschaften** zu öffnen, nehmen Sie an den entsprechenden Scan-Eigenschaften die gewünschten Änderungen vor und klicken Sie anschließend auf **Anwenden**, um Ihre Änderungen zu übernehmen.

Der Scan-Vorgang wird mit den neuen Einstellungen durchgeführt, wenn der nächste Anforderungsscan-Task gestartet wird. Wenn gerade ein Anforderungsscan-Vorgang ausgeführt wird, während Sie die Scan-Eigenschaften ändern, treten die neuen Einstellungen erst beim Starten des nächsten Anforderungsscan-Vorgangs in Kraft.

3 Wenn Sie die Prüfung der Scan-Statistiken beendet haben, klicken Sie auf **Schließen**.

Anzeigen des Aktivitätsprotokolls

Das Aktivitätsprotokoll für das Scannen auf Anforderung zeigt spezifische Details zum ausgeführten Scan-Vorgang an. In der Zusammenfassung werden beispielsweise die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Öffnen Sie die Aktivitätsprotokolldatei mit einer der folgenden Methoden:

- Markieren Sie den Task und wählen Sie dann im Menü **Task** die Option **Aktivitätsprotokoll**.
- Klicken Sie mit der rechten Maustaste auf den Task in der Taskliste und wählen Sie die Option **Protokoll anzeigen**.

3 Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

Reaktionen auf die Erkennung von Viren

Der Anforderungsscanner sucht auf der Grundlage der von Ihnen im Dialogfeld **Scannen auf Anforderung – Eigenschaften** ausgewählten Konfigurationseinstellungen nach Viren. Weitere Informationen finden Sie unter *Konfigurieren von Anforderungstasks* auf Seite 99.

Wenn ein Virus gefunden wird, erhalten Sie eine Benachrichtigung, falls Sie den Warnungs-Manager und/oder den Zugriffsscanner so konfiguriert haben, dass bei der Erkennung eines Virus eine Nachricht an Sie gesendet werden soll.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Empfangen von Benachrichtigungen über die Erkennung von Viren
- Durchführen von Aktionen bei einer Viruserkennung

Empfangen von Benachrichtigungen über die Erkennung von Viren

Der Anforderungsscanner kann drei Arten von Benachrichtigungen senden, wenn er einen Virus findet:

- **VirusScan-Warnung**: Bei Erkennung eines Virus wird ein Warnungsdialogfeld angezeigt, falls Sie für den Anforderungsscanner auf der Registerkarte **Aktionen** die Option **Aktion anfordern** als primäre oder sekundäre Aktion festgelegt haben. Weitere Informationen finden Sie unter *Aktionseigenschaften* auf Seite 110.

  Weitere Informationen über das Dialogfeld **VirusScan-Warnung** finden Sie unter *Durchführen von Aktionen bei einer Viruserkennung* auf Seite 123.

- **Messenger-Dienst**: Wenn Sie den Warnungs-Manager entsprechend konfiguriert haben, wird eine Netzwerkmeldung angezeigt. Weitere Informationen finden Sie unter *Konfigurieren des Warnungs-Managers* auf Seite 162.

  Nachstehend finden Sie ein Beispiel für eine vom Warnungs-Manager versendete Netzwerknachricht.

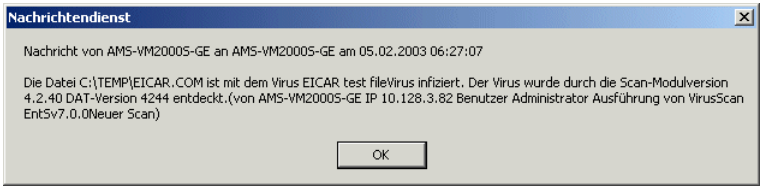

Nachrichtendienst
Nachricht von AMS-VM2000S-GE an AMS-VM2000S-GE am 05.02.2003 06:27:07
Die Datei C:\TEMP\EICAR.COM ist mit dem Virus EICAR test fileVirus infiziert. Der Virus wurde durch die Scan-Modulversion 4.2.40 DAT-Version 4244 entdeckt.(von AMS-VM2000S-GE IP 10.128.3.82 Benutzer Administrator Ausführung von VirusScan EntSv7.0.0Neuer Scan)
OK

Abbildung 4-16. Scannen auf Anforderung – Messenger-Dienst

  Die Meldung enthält Details zur infizierten Datei, wie beispielsweise den Dateinamen, den Speicherort der Datei, den Typ der erkannten Viren sowie die Version des Scan-Moduls und der DAT-Datei, die zur Erkennung des Virus verwendet wurde. Rufen Sie die Meldungsdetails auf und klicken Sie anschließend auf **OK**, um die Meldung zu schließen.

- **Status des Scannens auf Anforderung**: Das Dialogfeld **Status des Scannens auf Anforderung** wird angezeigt, während der Anforderungsscanner einen Task ausführt. Wenn Infektionen gefunden werden, werden sie im unteren Bereich des Dialogfelds angezeigt. Weitere Informationen finden Sie unter *Dialogfeld "Status des Scannens auf Anforderung"* auf Seite 124.

Je nachdem, wie Sie den Warnungs-Manager und den Anforderungsscanner konfiguriert haben, erhalten Sie möglicherweise mehrere Benachrichtigungen.

HINWEIS
Sie erhalten keine **VirusScan-Warnung** oder Netzwerkmeldung, wenn Sie dies nicht explizit im Anforderungsscanner oder Warnungs-Manager festgelegt haben. Sie können die erkannten Viren jedoch bei einem Scan-Vorgang immer im Dialogfeld **Status des Scannens auf Anforderung** sehen.

Durchführen von Aktionen bei einer Viruserkennung

Dieser Abschnitt beschreibt die Aktionen, die Sie durchführen können, wenn der Anforderungsscanner einen Virus erkennt.

HINWEIS
Sie haben außerdem die Möglichkeit, ein Virusbeispiel zur Analyse an AVERT zu senden. Weitere Informationen finden Sie unter *Einsenden eines Virenbeispiels* auf Seite 41.

Je nachdem, wie Sie über die Viruserkennung benachrichtigt wurden, legen Sie im Dialogfeld **VirusScan-Warnung** oder im Dialogfeld **Status des Scannens auf Anforderung** die Aktion fest, die für den gefundenen Virus ausgeführt werden soll.

- Wenn Sie durch eine **VirusScan-Warnung** benachrichtigt wurden, wählen Sie die Aktion in diesem Dialogfeld.
- Wenn Sie im Dialogfeld **Status des Scannens auf Anforderung** über den Virus informiert wurden, wählen Sie dort die entsprechende Aktion.

Dialogfeld "VirusScan-Warnung"

Das Dialogfeld **VirusScan-Warnung** wird angezeigt, um Sie über eine Viruserkennung zu informieren, wenn Sie den Anforderungsscanner mit der Option **Aktion anfordern** konfiguriert haben. Es enthält Informationen darüber, wo sich die gefundene Datei befindet und welcher Virustyp in der Datei gefunden wurde.

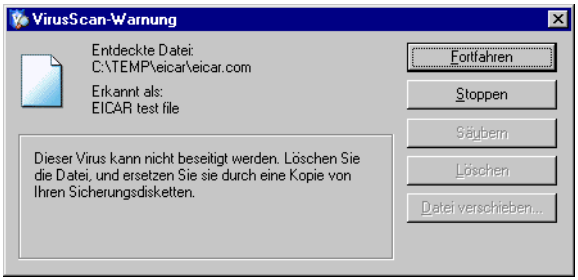


Abbildung 4-17. VirusScan-Warnung

Wählen Sie eine Aktion aus, die an der infizierten Datei durchgeführt werden soll:

- **Fortfahren**: Setzt den Scan-Vorgang fort, zeichnet jede Erkennung im Aktivitätsprotokoll auf und listet alle infizierten Dateien im Dialogfeld **Scannen auf Anforderung** auf.
- **Stoppen**: Stoppt den Scan-Vorgang sofort.
- **Säubern**: Versucht, die in der gewählten Meldung angegebene Datei zu säubern.

  Wenn die Datei nicht gesäubert werden kann, weil keine Säuberungsfunktion vorhanden ist oder weil der Virus die Datei so beschädigt hat, dass sie nicht gesäubert werden kann, wird ein Eintrag in der Protokolldatei aufgezeichnet. Möglicherweise werden alternative Aktionen vorgeschlagen. Wenn eine Datei z. B. nicht gesäubert werden kann, sollten Sie die Datei löschen und aus einer Sicherungskopie wiederherstellen.
- **Löschen**: Löscht die in der gewählten Meldung angegebene Datei. Der Dateiname wird im Protokoll aufgezeichnet, so dass Sie die Datei aus einer Sicherungskopie wiederherstellen können.
- **Datei verschieben**: Verschiebt die in der gewählten Meldung angegebene Datei in den Ordner, den Sie in dem Dialogfeld ausgewählt haben.

Dialogfeld "Status des Scannens auf Anforderung"

Das Dialogfeld **Status des Scannens auf Anforderung** wird angezeigt, während der Anforderungsscanner Tasks ausführt. Der untere Bereich zeigt Viren an, die während des Anforderungsscan-Vorgangs gefunden wurden.

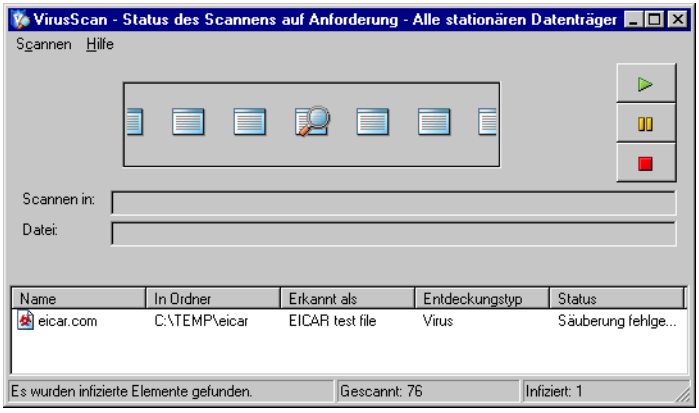


Abbildung 4-18. Status des Scannens auf Anforderung – Virus entdeckt

1 Führen Sie eine der folgenden Aktionen für den gefundenen Virus aus:

- Klicken Sie mit der rechten Maustaste auf den Dateinamen im unteren Fensterbereich und wählen Sie aus dem Menü die Aktion aus, die Sie ausführen möchten.
- Markieren Sie den Dateinamen im unteren Fensterbereich und wählen Sie aus dem Menü **Scannen** die Aktion aus, die Sie ausführen möchten.

2 Wenn Sie keine Aktionen für die in der Liste angezeigten Viren mehr ausführen möchten, wählen Sie im Menü **Scannen** den Befehl **Beenden**, um das Dialogfeld zu schließen.

Scannen von E-Mails 5

Der E-Mail-Scanner bietet Ihnen zwei Möglichkeiten zum Scannen von E-Mail-Dateien, Ordnern, Anlagen und Nachrichtentexten für einen lokalen oder Remote-Host:

- Der E-Mail-Empfangsscanner überprüft E-Mail-Nachrichten und Anlagen beim Empfang, wenn Microsoft Outlook ausgeführt wird. Sie können den E-Mail-Empfangsscanner über die **VirusScan-Konsole** konfigurieren und ausführen.
- Der E-Mail-Anforderungsscanner überprüft E-Mail-Nachrichten und Anlagen über Microsoft Outlook nach Bedarf. Sie können den E-Mail-Empfangsscanner von Microsoft Outlook aus konfigurieren und ausführen.

  Verwenden Sie den E-Mail-Anforderungsscanner, um den Schutz zu erweitern, den der E-Mail-Empfangsscanner bietet. Wenn z. B. Microsoft Outlook nicht gestartet wurde oder VirusScan Enterprise zum ersten Mal installiert wird, sollten Sie zunächst einen E-Mail-Anforderungsscan ausführen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- E-Mail-Empfangsscan
- E-Mail-Scan auf Anforderung

E-Mail-Empfangsscan

Der E-Mail-Empfangsscanner überprüft E-Mail-Anlagen und Nachrichtentexte, wenn sie bei Microsoft Outlook eingehen.

HINWEIS
Der Empfangsscanner scannt jedoch keine E-Mail-Nachrichten, die eingehen, wenn Microsoft Outlook offline ist. Wenn Microsoft Outlook offline war, sollten Sie, nachdem Outlook erneut online ist, sobald wie möglich einen E-Mail-Anforderungsscan ausführen. Ausführliche Anweisungen dazu finden Sie unter *E-Mail-Scan auf Anforderung* auf Seite 144.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Konfigurieren des E-Mail-Scans bei Empfang für einen lokalen oder Remote-Host
- Anzeigen der Eigenschaften des E-Mail-Scans bei Empfang
- Anzeigen der Ergebnisse des E-Mail-Scans bei Empfang

Konfigurieren des E-Mail-Scans bei Empfang für einen lokalen oder Remote-Host

So konfigurieren Sie den **E-Mail-Scan** für einen lokalen oder Remote-Host in der **VirusScan-Konsole**:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

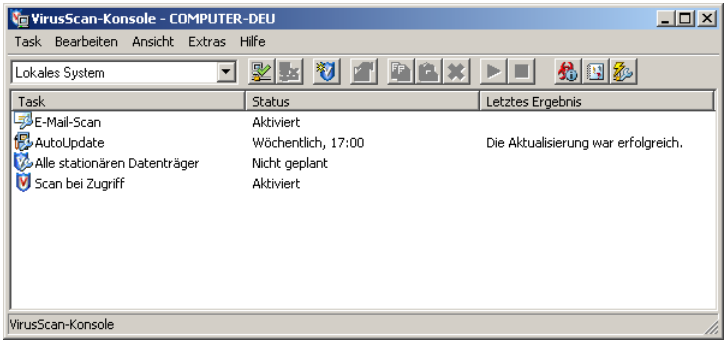


Abbildung 5-1. VirusScan-Konsole

Wenn Sie den **E-Mail-Scan** für einen lokalen Host konfigurieren, überspringen Sie Schritt 2 und fahren mit *Anzeigen der Eigenschaften des E-Mail-Scans bei Empfang* auf Seite 129 fort.

2 So konfigurieren Sie den **E-Mail-Scan** für einen Remote-Host:

a Wählen Sie aus dem Menü **Extras** die Option **Remote-Verbindung**.

b Geben Sie den Computernamen ein oder klicken Sie auf **Durchsuchen**, um den Pfad einzustellen.

c Klicken Sie auf **OK**, um zur **VirusScan-Konsole** zurückzukehren.

Anzeigen der Eigenschaften des E-Mail-Scans bei Empfang

Sie können den E-Mail-Scan bei Empfang so konfigurieren, dass E-Mails überprüft werden, wenn sie bei Microsoft Outlook eintreffen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Erkennungseigenschaften
- Erweiterte Eigenschaften
- Aktionseigenschaften
- Warnungseigenschaften
- Berichtseigenschaften

Erkennungseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erkennung**, um festzulegen, welche Anlagen und Dateinamenerweiterungen gescannt werden sollen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Empfang** mithilfe einer der folgenden Methoden:

- Markieren Sie in der Taskliste **E-Mail-Scan** und klicken Sie auf  .
- Klicken Sie mit der rechten Maustaste in der Taskliste auf **E-Mail-Scan** und wählen Sie anschließend **Eigenschaften**.
- Doppelklicken Sie in der Taskliste auf **E-Mail-Scan**.

HINWEIS
Wenn Outlook nicht konfiguriert wurde, wird das Dialogfeld für die Outlook-Konfiguration aufgerufen. Wenn Sie sich noch nicht beim Posteingang angemeldet haben, werden Sie jetzt dazu aufgefordert.

2 Wählen Sie die Registerkarte **Erkennung**.

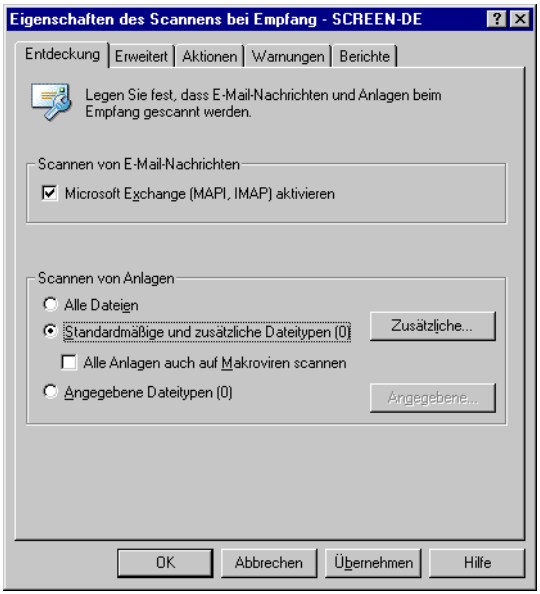


Abbildung 5-2. Eigenschaften des Scannens bei Empfang – Registerkarte "Erkennung"

3 Unter **Scannen von E-Mail-Nachrichten** ist die Option **Microsoft Exchange (MAPI, IMAP) aktivieren** *standardmäßig ausgewählt*. Zum Scannen von E-Mail-Nachrichten müssen Sie diese Option deaktivieren.

4 Wählen Sie unter **Scannen von Anlagen** eine dieser Optionen aus:

- **Alle Dateitypen**: *Diese Option ist standardmäßig ausgewählt*. Alle Anlagen werden unabhängig von der Erweiterung gescannt.
- **Standardmäßige und zusätzliche Dateitypen**: Die standardmäßig aufgelisteten Erweiterungen und alle zusätzlich angegebenen Dateitypen werden gescannt. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert. Sie können benutzerdefinierte Dateityperweiterungen hinzufügen und entfernen, aber keine Dateityperweiterungen aus der Standardliste löschen.

.

- **Ergänzungen**: Klicken Sie bei Auswahl von **Standardmäßige und zusätzliche Dateitypen** auf **Ergänzungen**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen von Dateityperweiterungen* auf Seite 75.

  Die Liste des E-Mail-Empfangsscanners kann maximal 1.000 zusätzliche Erweiterungen umfassen.

- **Alle Anlagen auch auf Makroviren scannen**: Alle Anlagen werden unabhängig von der Erweiterung auf Makroviren gescannt. Diese Option ist nur verfügbar, wenn die Option **Standardmäßige und zusätzliche Dateitypen** aktiviert ist.

  HINWEIS
  Ein Scan auf Makroviren in allen Anlagen könnte die Leistungsfähigkeit beeinträchtigen.

- **Angegebene Dateitypen**: Nur die von Ihnen angegebenen Dateitypen werden gescannt.

  - **Angegebene**: Klicken Sie bei Auswahl von **Angegebene Dateitypen** auf **Angegebene**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Die Liste der Dateityperweiterungen kann auch als Standardliste definiert werden. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen benutzerdefinierter Dateityperweiterungen* auf Seite 76.

    Die Liste des E-Mail-Empfangsscanners kann maximal 1.000 festgelegte Erweiterungen umfassen.

    HINWEIS
    Das Ausschließen von Dateitypen wird beim Scannen von E-Mail-Nachrichten nicht unterstützt.

5. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erweiterte Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erweitert**, um erweiterte Scan-Eigenschaften, z. B. Scannen nach unbekannten Programmviren und potenziell unerwünschten Programmen sowie von komprimierten Dateien und E-Mail-Nachrichtentexten festzulegen.

1. Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Empfang** mithilfe einer der folgenden Methoden:

   - Markieren Sie in der Taskliste **E-Mail-Scan** und klicken Sie auf  .

   - Klicken Sie mit der rechten Maustaste in der Taskliste auf **E-Mail-Scan** und wählen Sie anschließend **Eigenschaften**.

- Doppelklicken Sie in der Taskliste auf **E-Mail-Scan**.

  HINWEIS
  Wenn Outlook nicht konfiguriert wurde, wird das Dialogfeld für die Outlook-Konfiguration aufgerufen. Wenn Sie sich noch nicht beim Posteingang angemeldet haben, werden Sie jetzt dazu aufgefordert.

2 Wählen Sie die Registerkarte **Erweitert** aus.

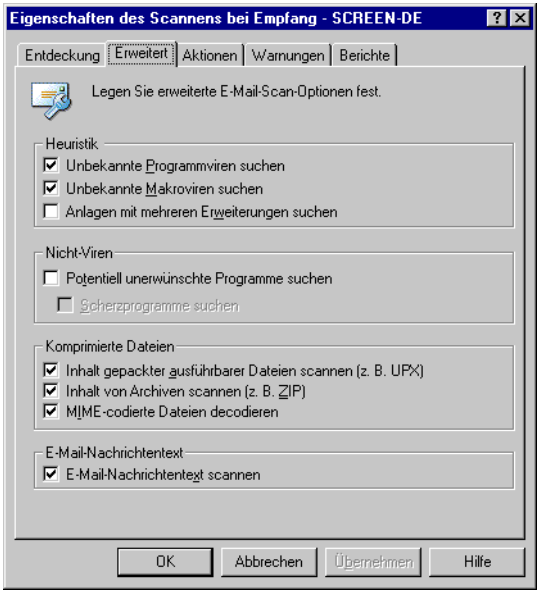


Abbildung 5-3. Eigenschaften des Scannens bei Empfang – Registerkarte "Erweitert"

3 Geben Sie unter **Heuristik** an, ob der Scanner die Wahrscheinlichkeit bewerten soll, mit der es sich bei unbekanntem Code oder Microsoft Office-Makros um Viren handelt. Wenn diese Funktion aktiviert ist, analysiert der Scanner, wie wahrscheinlich es ist, dass es sich hierbei um Varianten bekannter Viren handelt. Wählen Sie eine beliebige Kombination dieser Optionen:

- **Unbekannte Programmviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Ausführbare Dateien mit virenähnlichem Code werden wie infizierte Dateien behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion an.
- **Unbekannte Makroviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Eingebettete Makros mit virenähnlichem Code werden wie infizierte Makros behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

HINWEIS
Diese Option ist nicht mit der Option **Alle Dateien auch auf Makroviren scannen** auf der Registerkarte **Erkennung** identisch, mit der der Scanner nach allen bekannten Makroviren sucht. Mit dieser Option wird der Scanner angewiesen, die *Wahrscheinlichkeit* zu bewerten, mit der es sich bei einem unbekannten Makro um ein Virus handelt.

- **Anlagen mit mehreren Erweiterungen suchen**: Anlagen mit mehreren Erweiterungen werden wie infizierte Anlagen behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

  Bei Auswahl dieser Option wird das Dialogfeld **E-Mail-Scan-Warnung** angezeigt.

  - **E-Mail-Scan-Warnung**: Lesen Sie die Warnung sorgfältig durch. Klicken Sie auf **OK**, um fortzusetzen und die Auswahl zu akzeptieren und Anlagen mit mehreren Erweiterungen so zu behandeln, als wären sie infiziert, oder klicken Sie auf **Abbrechen**, um die Option zu deaktivieren.

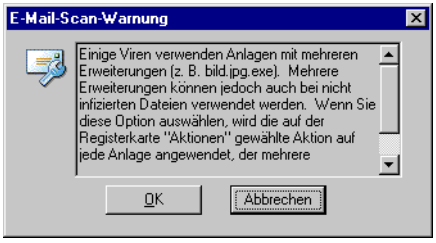

E-Mail-Scan-Warnung
Einige Viren verwenden Anlagen mit mehreren Erweiterungen (z. B. bild.jpg.exe). Mehrere Erweiterungen können jedoch auch bei nicht infizierten Dateien verwendet werden. Wenn Sie diese Option auswählen, wird die auf der Registerkarte "Aktionen" gewählte Aktion auf jede Anlage angewendet, der mehrere
OK
Abbrechen

Abbildung 5-4. E-Mail-Scan-Warnung

4 Geben Sie unter **Nicht-Viren** an, ob der Scanner nach potenziell unerwünschten Nicht-Viren-Anwendungen suchen soll.

- **Potenziell unerwünschte Programme suchen**: Potenziell unerwünschte Programme werden erkannt.

  - **Scherzviren suchen**: Wenn Sie die Option **Potenziell unerwünschte Programme suchen** gewählt haben, können Sie auch nach Scherzprogrammen suchen.

WARNUNG
VirusScan Enterprise unternimmt keine Maßnahmen gegen potenziell unerwünschte Programmdateien oder Scherzprogramme, die entdeckt werden. Erkennungen werden in der Protokolldatei protokolliert.

Wenn Sie bei einer erkannten, potenziell unerwünschten Programmdatei oder einem Scherzprogramm aktiv werden möchten, müssen Sie dies manuell tun. Wenn Sie z. B. ein erkanntes Scherzprogramm entfernen möchten, müssen Sie es manuell entfernen.

5 Wählen Sie unter **Komprimierte Dateien** aus, welche Typen von komprimierten Dateien vom Scanner überprüft werden sollen. Sie haben folgende Optionen:

- **Inhalt gepackter ausführbarer Dateien scannen**: *Diese Option ist standardmäßig ausgewählt.* Komprimierte Dateien mit ausführbaren Programmdateien werden überprüft. Eine verpackte Programmdatei wird beim Ausführen niemals auf einen Datenträger, sondern immer direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.
- **Inhalt von Archiven scannen**: *Diese Option ist standardmäßig ausgewählt.* Archivdateien und ihr Inhalt werden überprüft. Eine Archivdatei ist eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann. Die in Archiven enthaltenen Dateien werden gescannt, bevor Sie auf Datenträgern gespeichert werden.
- **MIME-codierte Dateien decodieren**: *Diese Option ist standardmäßig ausgewählt.* Multipurpose Internet Mail Extensions (MIME)-kodierte Dateien werden erkannt, dekodiert und dann gescannt.

  HINWEIS
  Das Scannen komprimierter Dateien verbessert zwar den Schutz, dafür kann sich jedoch auch die für den Scan-Vorgang benötigte Zeit erhöhen.

6 Unter **E-Mail-Nachrichtentext** ist die Option **E-Mail-Nachrichtentext scannen** *standardmäßig ausgewählt.* Wenn Sie die Auswahl dieser Option aufheben, werden E-Mail-Nachrichtentexte nicht gescannt.

7 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Aktionseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Aktionen**, um die primären und sekundären Aktionen festzulegen, die beim Erkennen eines Virus vom Scan-Programm ausgeführt werden sollen.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Empfang** mithilfe einer der folgenden Methoden:

- Markieren Sie in der Taskliste **E-Mail-Scan** und klicken Sie auf  .
- Klicken Sie mit der rechten Maustaste in der Taskliste auf **E-Mail-Scan** und wählen Sie anschließend **Eigenschaften**.
- Doppelklicken Sie in der Taskliste auf **E-Mail-Scan**.

HINWEIS
Wenn Outlook nicht konfiguriert wurde, wird das Dialogfeld für die Outlook-Konfiguration aufgerufen. Wenn Sie sich noch nicht beim Posteingang angemeldet haben, werden Sie jetzt dazu aufgefordert.

2 Wählen Sie die Registerkarte **Aktionen**.



Abbildung 5-5. Eigenschaften des Scannens bei Empfang – Registerkarte "Aktionen"

3 Wählen Sie unter **Wenn infizierte Anlagen gefunden werden** die primäre Aktion aus, die das Programm bei Erkennung eines Virus ausführen soll.

HINWEIS
Die primäre Standardaktion ist **Infizierte Anhänge säubern**.

Klicken Sie auf , um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Bei Erkennung eines Virus wird eine Eingabeaufforderung an den Benutzer ausgegeben.

  Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben Stoppen und Fortfahren noch zulässig sind. Folgende Optionen stehen zur Auswahl:

  - **Anhang säubern**: Der infizierte Anhang kann gesäubert werden.
  - **Anhang verschieben**: Der infizierte Anhang kann verschoben werden.
  - **Anhang löschen**: Der infizierte Anhang kann gelöscht werden.

  Für diese Option ist keine sekundäre Aktion zulässig.

- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung eines infizierten Anhangs fortgesetzt.

  Für diese Option ist keine sekundäre Aktion zulässig.

- **Infizierte Anhänge in Ordner verschieben**: Infizierte Anhänge werden in einen Quarantäneordner verschoben. Der Standardname des Quarantäneordners lautet *Quarantine*. Sie können den Standardnamen des Ordners übernehmen oder einen neuen Namen eingeben.

  HINWEIS
  Der *Quarantäneordner* wird in der MAPI-Datenbank erstellt und kann in Microsoft Outlook in der **Ordnerliste** angezeigt werden.

- **Infizierte Anhänge säubern**: *Diese Option ist standardmäßig ausgewählt.* Der Scanner versucht, den Virus aus dem infizierten Anhang zu entfernen. Wenn der Scanner den Virus nicht aus einem infizierten Anhang entfernen kann oder der Virus den Anhang irreparabel beschädigt hat, führt der Scanner die sekundäre Aktion aus.

- **Infizierte Anhänge löschen**: Infizierte Anhänge werden bei Erkennung sofort gelöscht. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Anhänge erfasst werden.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

4 Wählen Sie unter **Wenn die oben genannte Aktion fehlschlägt** die sekundäre Aktion aus, die das Scan-Programm beim Fehlschlagen der primären Aktion ausführen soll.

> **HINWEIS**
> Bei der sekundären Standardaktion handelt es sich um **Infizierte Anhänge in Ordner verschieben**.

Klicken Sie auf , um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Bei Erkennung eines Virus wird eine Eingabeaufforderung an den Benutzer ausgegeben.

  Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben Stoppen und Fortfahren noch zulässig sind. Folgende Optionen stehen zur Auswahl:

  - **Anhang säubern**: Der infizierte Anhang kann gesäubert werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang säubern** ausgewählt haben.
  - **Anhang verschieben**: Der infizierte Anhang kann verschoben werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang verschieben** ausgewählt haben.
  - **Anhang löschen**: Der infizierte Anhang kann gelöscht werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang löschen** ausgewählt haben.

- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung einer infizierten Datei fortgesetzt.
- **Infizierte Anhänge in Ordner verschieben**: *Diese Option ist standardmäßig ausgewählt.* Infizierte Anhänge werden in einen Quarantäneordner verschoben. Der Standardname des Quarantäneordners lautet *Quarantine*. Sie können den Standardnamen des Ordners übernehmen oder einen neuen Namen eingeben.

  > **HINWEIS**
  > Der *Quarantäneordner* wird in der MAPI-Datenbank erstellt und kann in Microsoft Outlook in der **Ordnerliste** angezeigt werden.

- **Infizierte Anhänge löschen**: Infizierte Anhänge werden bei Erkennung sofort gelöscht. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Anhänge erfasst werden.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Warnungseigenschaften

Wählen Sie die Optionen auf der Registerkarte **Warnungen**, um die Warnungen zu konfigurieren, die Benutzern bei Erkennung einer infizierten E-Mail-Nachricht bzw. eines Anhangs angezeigt werden.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Empfang** mithilfe einer der folgenden Methoden:

- Markieren Sie in der Taskliste **E-Mail-Scan** und klicken Sie auf  .
- Klicken Sie mit der rechten Maustaste in der Taskliste auf **E-Mail-Scan** und wählen Sie anschließend **Eigenschaften**.
- Doppelklicken Sie in der Taskliste auf **E-Mail-Scan**.

HINWEIS
Wenn Outlook nicht konfiguriert wurde, wird das Dialogfeld für die Outlook-Konfiguration aufgerufen. Wenn Sie sich noch nicht beim Posteingang angemeldet haben, werden Sie jetzt dazu aufgefordert.

2 Wählen Sie die Registerkarte **Warnungen** aus.

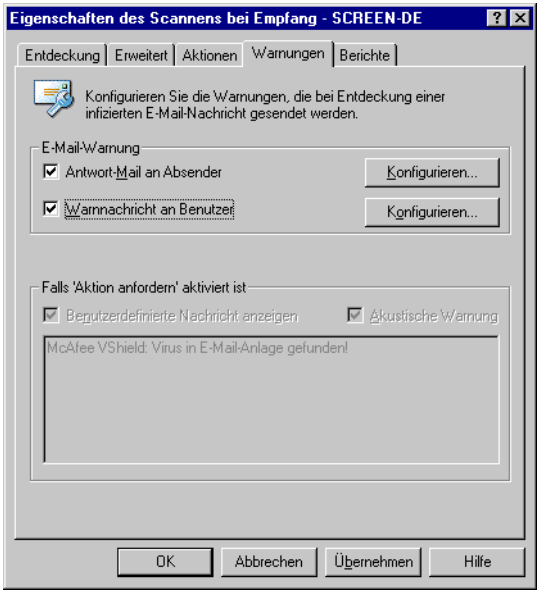


Abbildung 5-6. Eigenschaften des Scannens bei Empfang – Registerkarte "Warnungen"

3 Geben Sie unter **E-Mail-Warnung** an, wie Absender und Benutzer von E-Mails bei Erkennung einer infizierten Nachricht benachrichtigt werden sollen. Sie haben folgende Optionen:

- **Antwort-Mail an Absender**: An den Absender wird eine Antwort-Mail gesendet.
  - Wenn Sie diese Option wählen, müssen Sie auf **Konfigurieren** klicken, um das Dialogfeld **"E-Mail zurücksenden" konfigurieren** aufzurufen.

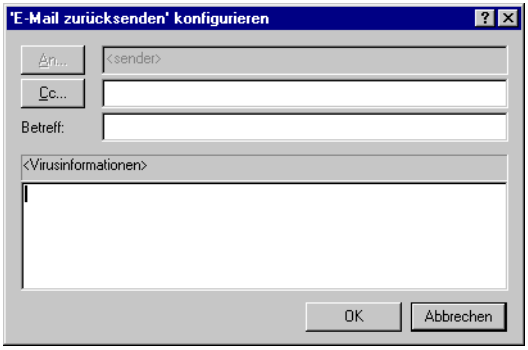


Abbildung 5-7. E-Mail-Scan – "E-Mail zurücksenden" konfigurieren

  - Geben Sie die Nachricht ein, die gesendet werden soll, und klicken Sie auf **OK**.

- **Warn-Mail an Benutzer senden**: Es wird eine Warn-E-Mail an einen Benutzer gesendet.
  - Wenn Sie diese Option gewählt haben, klicken Sie auf **Konfigurieren**, um das Dialogfeld **"E-Mail senden" konfigurieren** aufzurufen.

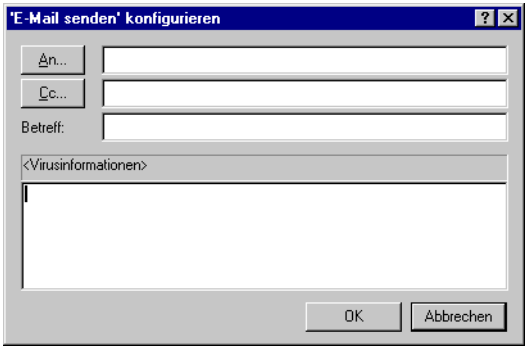


Abbildung 5-8. E-Mail-Scan – "E-Mail senden" konfigurieren

- Geben Sie die Nachricht ein, die gesendet werden soll, und klicken Sie auf **OK**.

4 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

5 Geben Sie unter **Falls "Aktion anfordern" aktiviert ist** an, wie die Benutzer bei Erkennung einer infizierten E-Mail benachrichtigt werden sollen. Sie haben folgende Optionen:

- **Benutzerdefinierte Nachricht anzeigen**: *Diese Option ist standardmäßig ausgewählt.* Der Benutzer erhält eine benutzerdefinierte Nachricht. Wenn Sie diese Option auswählen, können Sie eine benutzerdefinierte Nachricht in das Textfeld eingeben.
- **Akustische Warnung**: *Diese Option ist standardmäßig ausgewählt.* Der Benutzer wird durch ein akustisches Signal benachrichtigt.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Berichtseigenschaften

Klicken Sie auf die Registerkarte **Berichte**, um die Protokollierungsaktivitäten zu konfigurieren. Geben Sie den Speicherort und die Größe der Protokolldatei sowie die Informationen an, die Sie pro Protokolleintrag erfassen möchten.

HINWEIS
Die Protokolldatei ist ein wichtiges Verwaltungstool, mit dem Sie Virenaktivitäten im Netzwerk verfolgen und die vom Scanner zur Erkennung und Behandlung erkannter Viren verwendeten Einstellungen festhalten können. Anhand der in der Datei protokollierten Ereignisse können Sie feststellen, welche Dateien durch Sicherungskopien ersetzt, im Quarantäneordner geprüft oder vom Rechner gelöscht werden müssen. Weitere Informationen finden Sie unter *Anzeigen des Protokolls für E-Mail-Aktivitäten bei Empfang* auf Seite 144.

1 Öffnen Sie das Dialogfeld **Eigenschaften des Scannens bei Empfang** mithilfe einer der folgenden Methoden:

- Markieren Sie in der Taskliste **E-Mail-Scan** und klicken Sie auf  .
- Klicken Sie mit der rechten Maustaste in der Taskliste auf **E-Mail-Scan** und wählen Sie anschließend **Eigenschaften**.
- Doppelklicken Sie in der Taskliste auf **E-Mail-Scan**.

HINWEIS
Wenn Outlook nicht konfiguriert wurde, wird das Dialogfeld für die Outlook-Konfiguration aufgerufen. Wenn Sie sich noch nicht beim Posteingang angemeldet haben, werden Sie jetzt dazu aufgefordert.

2 Wählen Sie die Registerkarte **Berichte**.

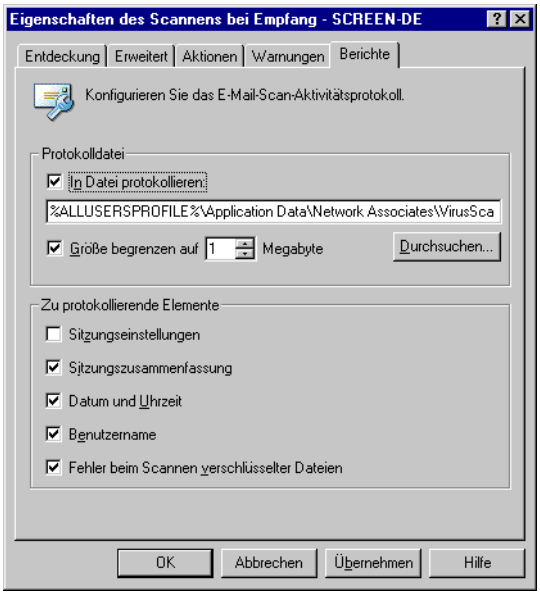


Abbildung 5-9. Eigenschaften des Scannens bei Empfang – Registerkarte "Berichte"

3 Wählen Sie unter **Protokolldatei** eine dieser Optionen:

- **In Datei protokollieren**: *Diese Option ist standardmäßig ausgewählt.* Virusaktivitäten werden beim Scannen bei Empfang in einer Protokolldatei aufgezeichnet.
- Sie können den im Textfeld angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einer anderen geeigneten Datei auf dem Computer oder im Netzwerk zu wechseln.

  HINWEIS
  Standardmäßig schreibt der Scanner Protokollinformationen in die Datei EMAILONDELIVERYLOG.TXT in diesem Ordner:

  ```
  <Laufwerk>:Winnt\Profiles\All Users\Application
  Data\Network Associates\VirusScan
  ```

- **Größe begrenzen auf**: *Diese Option ist standardmäßig ausgewählt. Die Standardgröße der Protokolldatei ist 1 MB.* Übernehmen Sie die Standardgröße, oder legen Sie einen anderen Wert für die Protokolldatei fest. Wenn Sie diese Option auswählen, geben Sie einen Wert zwischen 1 MB und 999 MB ein.

HINWEIS
Wenn die Datenmenge in der Protokolldatei die von Ihnen festgelegte Dateigröße übersteigt, werden 20 Prozent der Protokolldateieinträge (die ältesten) gelöscht und der Datei neue Daten hinzugefügt.

4 Legen Sie unter **Zu protokollierende Elemente** fest, welche zusätzlichen Informationen in der Protokolldatei aufgezeichnet werden sollen:

- **Sitzungseinstellungen**: In der Protokolldatei werden die für die einzelnen Scan-Sitzungen ausgewählten Eigenschaften erfasst.
- **Sitzungszusammenfassung** *Diese Option ist standardmäßig ausgewählt.* Die Aktionen des Scanners bei den einzelnen Scan-Sitzungen werden zusammengefasst und der Protokolldatei hinzugefügt. Zu den Zusammenfassungsinformationen gehören die Anzahl der gescannten Dateien, Anzahl und Typ der entdeckten Viren, die Anzahl der verschobenen, gelöschten oder bereinigten Dateien sowie weitere Informationen.
- **Datum und Uhrzeit**: *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden Datum und Uhrzeit der Erkennung eines Virus erfasst.
- **Benutzername** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei wird der Name des Benutzers erfasst, der zum Zeitpunkt der Aufzeichnung der jeweiligen Protokolleinträge bei der E-Mail-Anwendung angemeldet war.
- **Fehler beim Scannen verschlüsselter Dateien**: *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden die Namen der verschlüsselten Dateien erfasst, die nicht gescannt werden konnten.

5 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Anzeigen der Ergebnisse des E-Mail-Scans bei Empfang

Sie können die Ergebnisse Ihrer Scan-Operationen in der statistischen Übersicht sowie im Aktivitätsprotokoll anzeigen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Anzeigen der Statistik des E-Mail-Scans bei Empfang
- Anzeigen des Protokolls für E-Mail-Aktivitäten bei Empfang

Anzeigen der Statistik des E-Mail-Scans bei Empfang

In der Zusammenfassung **Statistik für das Scannen von E-Mails mit VirusScan beim Empfang** werden die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Rufen Sie mit einer dieser Methoden das Dialogfeld **Statistik für das Scannen von E-Mails mit VirusScan beim Empfang** auf:

- Markieren Sie den E-Mail-Scan-Task in der Taskliste und wählen Sie dann aus dem Menü **Task** die Option **Statistik**.
- Klicken Sie mit der rechten Maustaste in der Taskliste auf den E-Mail-Scan-Task und wählen Sie anschließend **Statistik**.

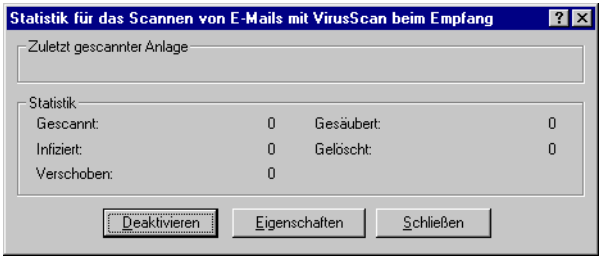


Abbildung 5-10. Statistik für das Scannen von E-Mails mit VirusScan beim Empfang

Im Dialogfeld **Statistik für das Scannen von E-Mails mit VirusScan beim Empfang** wird im oberen Bereich der **Zuletzt gescannte Anhang** angezeigt, während der untere Bereich eine statistische Übersicht enthält.

Wenn der Scan-Vorgang noch nicht abgeschlossen ist, werden die aktuell überprüfte Datei sowie der Status des Scan-Vorgangs angezeigt.

3 Sie können eine dieser Funktionen ausführen, wenn Sie über Administratorrechte verfügen und gegebenenfalls das Kennwort eingeben.

- Klicken Sie auf **Deaktivieren**, um den E-Mail-Empfangsscanner zu deaktivieren. Mit dieser Funktion schalten Sie zwischen **Aktivieren** und **Deaktivieren** um.
- Klicken Sie auf **Eigenschaften**, um das Dialogfeld **Eigenschaften des Scannens bei Empfang** zu öffnen, nehmen Sie an den entsprechenden Scan-Eigenschaften die gewünschten Änderungen vor und klicken Sie anschließend auf **Anwenden**, um Ihre Änderungen zu übernehmen.

  Die von Ihnen festgelegten neuen Einstellungen für Scan-Vorgänge werden sofort wirksam.

4 Wenn Sie die Anzeige der Scan-Statistiken beendet haben, klicken Sie auf **Schließen**.

Anzeigen des Protokolls für E-Mail-Aktivitäten bei Empfang

Das Aktivitätsprotokoll für das Scannen bei Empfang zeigt spezifische Details zum ausgeführten Scan-Vorgang an. In der Zusammenfassung werden beispielsweise die Anzahl der vom Scanner überprüften Dateien, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Öffnen Sie die Aktivitätsprotokolldatei mit einer der folgenden Methoden:

- Markieren Sie den E-Mail-Scan-Task und wählen Sie dann im Menü **Task** die Option **Aktivitätsprotokoll**.
- Klicken Sie mit der rechten Maustaste in der Taskliste auf den E-Mail-Scan-Task und wählen Sie anschließend **Protokoll anzeigen**.

3 Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

E-Mail-Scan auf Anforderung

Der E-Mail-Scan-Task auf Anforderung kann direkt über Microsoft Outlook zum Scannen von Nachrichten und Anlagen nach Bedarf ausgeführt werden. Verwenden Sie den E-Mail-Anforderungsscanner als Ergänzung zum E-Mail-Empfangsscanner, nachdem Microsoft Outlook nach einer längeren Zeit wieder geöffnet wird.

HINWEIS
Wenn Microsoft Outlook während der VirusScan Enterprise-Installation geöffnet war, wird empfohlen, Microsoft Outlook nach Abschluss des Installationsvorgangs neu zu starten.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Konfigurieren des E-Mail-Anforderungstasks
- Ausführen des E-Mail-Anforderungstasks
- Anzeigen der Ergebnisse des E-Mail-Anforderungsscans

Konfigurieren des E-Mail-Anforderungstasks

Für die Konfiguration des E-Mail-Scan-Tasks auf Anforderung, mit dem Nachrichten und Anlagen überprüft werden, können Sie Microsoft Outlook verwenden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Erkennungseigenschaften
- Erweiterte Eigenschaften
- Aktionseigenschaften
- Warnungseigenschaften
- Berichtseigenschaften

Erkennungseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erkennung**, um festzulegen, welche Anlagen und Dateinamenerweiterungen gescannt werden sollen.

1. Starten Sie Microsoft Outlook.
2. Rufen Sie das Dialogfeld **Eigenschaften des E-Mail-Scannens auf Anforderung** mit einer dieser Verfahrensweisen auf:
   - Wählen Sie im Menü **Extras** die Option **E-Mail-Scan-Eigenschaften**.
   - Klicken Sie in der Symbolleiste von Outlook auf  .

     HINWEIS
     Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard* -Symbolleiste auf  und Sie wählen dann das Symbol.
3. Wählen Sie die Registerkarte **Erkennung**.

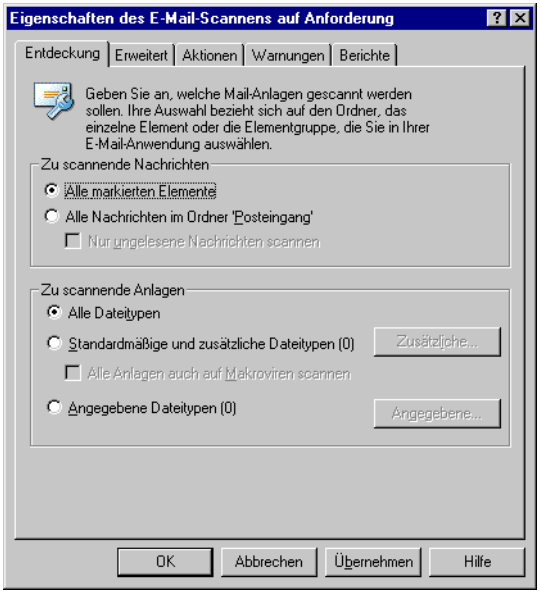


Abbildung 5-11. Eigenschaften des E-Mail-Scannens auf Anforderung – Registerkarte "Erkennung"

4 Geben Sie unter **Zu scannende Nachrichten** an, welche Nachrichten überprüft werden sollen. Sie haben folgende Optionen:

- **Alle markierten Elemente**: *Diese Option ist standardmäßig ausgewählt.* Ausgewählte E-Mail-Nachrichten oder -Ordner werden überprüft.
- **Alle Nachrichten im Ordner "Posteingang"**: Alle Nachrichten, die sich aktuell im Ordner **Posteingang** befinden, werden überprüft.
  - **Nur ungelesene Nachrichten scannen**: Es werden nur die ungelesenen Nachrichten im Ordner **Posteingang** und in seinen Unterordnern überprüft. Wenn **Alle Nachrichten im Ordner "Posteingang"** nicht aktiviert wurde, ist diese Option deaktiviert.

5 Geben Sie unter **Zu scannende Anlagen** an, welche Dateien, Ordner oder Laufwerke überprüft werden sollen. Sie haben folgende Optionen:

- **Alle Dateitypen**: *Diese Option ist standardmäßig ausgewählt.* Alle Anlagen werden unabhängig von der Erweiterung gescannt.
- **Standardmäßige und zusätzliche Dateitypen**: Die standardmäßig aufgelisteten Erweiterungen und alle zusätzlich angegebenen Dateitypen werden gescannt. Die Standardliste der Dateityperweiterungen wird durch die aktuelle DAT-Datei definiert. Sie können benutzerdefinierte Dateityperweiterungen hinzufügen und entfernen, aber keine Dateityperweiterungen aus der Standardliste löschen.
  - **Ergänzungen**: Klicken Sie bei Auswahl von **Standardmäßige und zusätzliche Dateitypen** auf **Ergänzungen**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen von Dateityperweiterungen* auf Seite 75.

    Die Liste des E-Mail-Anforderungsscanners kann maximal 1.000 zusätzliche Erweiterungen umfassen.
  - **Alle Anlagen auch auf Makroviren scannen**: Alle Anlagen werden unabhängig von der Erweiterung auf Makroviren gescannt. Diese Option ist nur verfügbar, wenn die Option **Standardmäßige und zusätzliche Dateitypen** aktiviert ist.

    HINWEIS
    Ein Scan auf Makroviren in allen Anlagen könnte die Leistungsfähigkeit beeinträchtigen.
- **Angegebene Dateitypen**: Nur die von Ihnen angegebenen Dateitypen werden gescannt.
  - **Angegebene**: Klicken Sie bei Auswahl von **Angegebene Dateitypen** auf **Angegebene**, um benutzerdefinierte Dateityperweiterungen hinzuzufügen oder zu entfernen. Die Liste der Dateityperweiterungen kann auch als Standardliste definiert werden. Ausführliche Anweisungen dazu finden Sie unter *Hinzufügen benutzerdefinierter Dateityperweiterungen* auf Seite 76.

    Die Liste des E-Mail-Anforderungsscanners kann maximal 1.000 Erweiterungen umfassen.

    HINWEIS
    Das Ausschließen von Dateitypen wird beim Scannen von E-Mail-Nachrichten nicht unterstützt.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Erweiterte Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Erweitert**, um erweiterte Scan-Eigenschaften wie z. B. Scannen nach unbekannten Programmviren und potenziell unerwünschten Programmen sowie von komprimierten Dateien und E-Mail-Nachrichtentexten festzulegen.

1. Starten Sie Microsoft Outlook.
2. Rufen Sie das Dialogfeld **Eigenschaften des E-Mail-Scannens auf Anforderung** mit einer dieser Verfahrensweisen auf:
   - Wählen Sie aus dem Menü **Extras** die Option **E-Mail-Scan-Eigenschaften**.
   - Klicken Sie in der Symbolleiste von Outlook auf  .

     HINWEIS
     Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard*-Symbolleiste auf  und wählen dann das Symbol.
3. Wählen Sie die Registerkarte **Erweitert** aus.

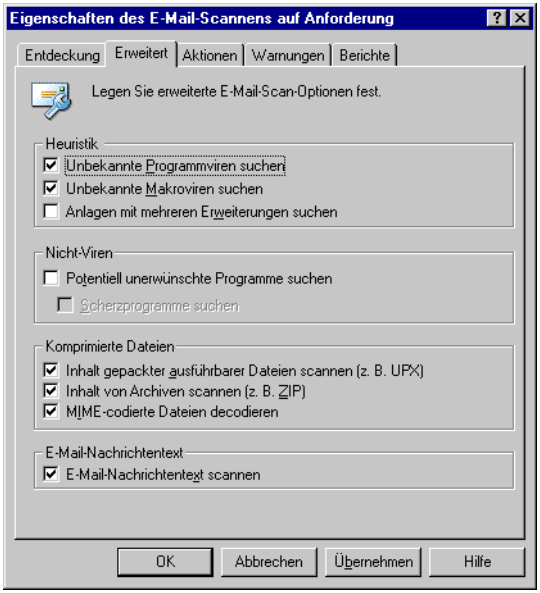


Abbildung 5-12. Eigenschaften des E-Mail-Scannens auf Anforderung – Registerkarte "Erweitert"

4 Geben Sie unter **Heuristik** an, ob der Scanner die Wahrscheinlichkeit bewerten soll, mit der es sich bei unbekanntem Code oder Microsoft Office-Makros um Viren handelt. Wenn diese Funktion aktiviert ist, analysiert der Scanner, wie wahrscheinlich es ist, dass es sich hierbei um Varianten bekannter Viren handelt. Sie haben folgende Optionen:

- **Unbekannte Programmviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Ausführbare Dateien mit virenähnlichem Code werden wie infizierte Dateien behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.
- **Unbekannte Makroviren suchen**: *Diese Option ist standardmäßig ausgewählt.* Eingebettete Makros mit virenähnlichem Code werden wie infizierte Makros behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

  HINWEIS
  Diese Option ist nicht mit der Option **Alle Dateien auch auf Makroviren scannen** auf der Registerkarte **Erkennung** identisch, mit der der Scanner nach allen bekannten Makroviren sucht. Mit dieser Option wird der Scanner angewiesen, die *Wahrscheinlichkeit* zu bewerten, mit der es sich bei einem unbekannten Makro um ein Virus handelt.

- **Anlagen mit mehreren Erweiterungen suchen**: Anlagen mit mehreren Erweiterungen werden wie infizierte Anlagen behandelt. Der Scanner wendet die von Ihnen auf der Registerkarte **Aktionen** festgelegte Aktion auf diese Dateien an.

  Bei Auswahl dieser Option wird das Dialogfeld **E-Mail-Scan-Warnung** angezeigt.

  - **E-Mail-Scan-Warnung**: Lesen Sie die Warnung sorgfältig durch. Klicken Sie auf **OK**, um fortzusetzen und die Auswahl zu akzeptieren und Anlagen mit mehreren Erweiterungen so zu behandeln, als wären sie infiziert, oder klicken Sie auf **Abbrechen**, um die Option zu deaktivieren.

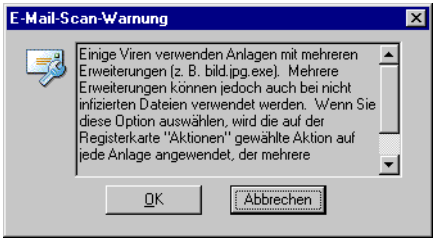

E-Mail-Scan-Warnung
Einige Viren verwenden Anlagen mit mehreren Erweiterungen (z. B. bild.jpg.exe). Mehrere Erweiterungen können jedoch auch bei nicht infizierten Dateien verwendet werden. Wenn Sie diese Option auswählen, wird die auf der Registerkarte "Aktionen" gewählte Aktion auf jede Anlage angewendet, der mehrere
OK
Abbrechen

Abbildung 5-13. E-Mail-Scan-Warnung

5 Geben Sie unter **Nicht-Viren** an, ob der Scanner nach potenziell unerwünschten Nicht-Viren-Anwendungen suchen soll.

- **Potenziell unerwünschte Programme suchen**: Potenziell unerwünschte Programme werden erkannt.
  - **Scherzviren suchen**: Wenn Sie die Option **Potenziell unerwünschte Programme suchen** gewählt haben, können Sie auch nach Scherzprogrammen suchen.

    WARNUNG
    VirusScan Enterprise unternimmt keine Maßnahmen gegen potenziell unerwünschte Programmdateien oder Scherzprogramme. Erkennungen werden in der Protokolldatei protokolliert.

6 Wählen Sie unter **Komprimierte Dateien** aus, welche Typen von komprimierten Dateien vom Scanner überprüft werden sollen. Sie haben folgende Optionen:

- **Inhalt gepackter ausführbarer Dateien scannen**: *Diese Option ist standardmäßig ausgewählt.* Komprimierte Dateien mit ausführbaren Programmdateien werden überprüft. Eine verpackte Programmdatei wird beim Ausführen niemals auf einen Datenträger, sondern immer direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.
- **Inhalt von Archiven scannen**: *Diese Option ist standardmäßig ausgewählt.* Archivdateien und ihr Inhalt werden überprüft. Eine Archivdatei ist eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann. Die in Archiven enthaltenen Dateien werden gescannt, bevor Sie auf Datenträgern gespeichert werden.
- **MIME-codierte Dateien decodieren**: *Diese Option ist standardmäßig ausgewählt.* Multipurpose Internet Mail Extensions (MIME)-kodierte Dateien werden erkannt, dekodiert und dann gescannt.

  HINWEIS
  Das Scannen komprimierter Dateien verbessert zwar den Schutz, dafür kann sich jedoch auch die für den Scan-Vorgang benötigte Zeit erhöhen.

7 Unter **E-Mail-Nachrichtentext** ist die Option **E-Mail-Nachrichtentext scannen** *standardmäßig ausgewählt.* Wenn Sie die Auswahl dieser Option aufheben, werden E-Mail-Nachrichtentexte nicht gescannt.

8 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Aktionseigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Aktionen**, um die primären und sekundären Aktionen festzulegen, die beim Erkennen eines Virus vom Scan-Programm ausgeführt werden sollen.

1 Starten Sie Microsoft Outlook.

2 Rufen Sie das Dialogfeld **Eigenschaften des E-Mail-Scannens auf Anforderung** mit einer dieser Verfahrensweisen auf:

- Wählen Sie aus Menü **Extras** die Option **E-Mail-Scan-Eigenschaften**.
- Klicken Sie in der Symbolleiste von Outlook auf .

HINWEIS
Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard*-Symbolleiste auf und wählen dann das Symbol.

3 Wählen Sie die Registerkarte **Aktionen**.

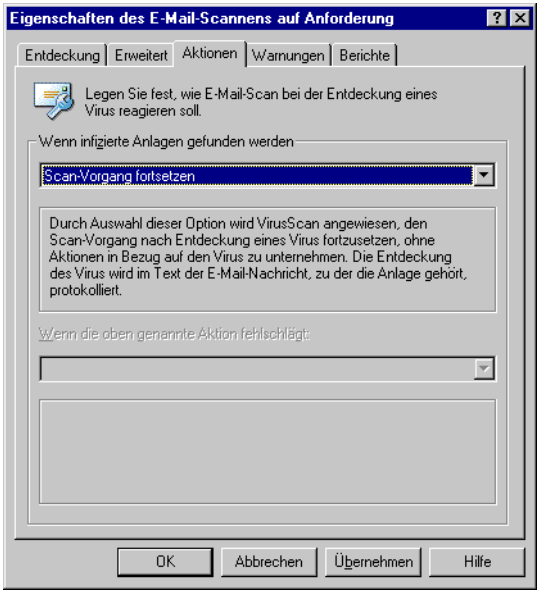

Eigenschaften des E-Mail-Scannens auf Anforderung
Entdeckung
Erweitert
Aktionen
Warnungen
Berichte
Legen Sie fest, wie E-Mail-Scan bei der Entdeckung eines Virus reagieren soll.
Wenn infizierte Anlagen gefunden werden
Scan-Vorgang fortsetzen
Durch Auswahl dieser Option wird VirusScan angewiesen, den Scan-Vorgang nach Entdeckung eines Virus fortzusetzen, ohne Aktionen in Bezug auf den Virus zu unternehmen. Die Entdeckung des Virus wird im Text der E-Mail-Nachricht, zu der die Anlage gehört, protokolliert.
Wenn die oben genannte Aktion fehlschlägt:
OK
Abbrechen
Übernehmen
Hilfe

Abbildung 5-14. Eigenschaften des E-Mail-Scannens auf Anforderung – Registerkarte "Aktionen"

4 Wählen Sie unter **Wenn infizierte Anlagen gefunden werden** die primäre Aktion aus, die das Programm bei Erkennung eines Virus ausführen soll.

HINWEIS
Die primäre Standardaktion ist **Infizierte Anhänge säubern**.

Klicken Sie auf , um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Bei Erkennung eines Virus wird eine Eingabeaufforderung an den Benutzer ausgegeben.

  Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben Stoppen und Fortfahren noch zulässig sind. Folgende Optionen stehen zur Auswahl:

  - **Anhang säubern**: Der infizierte Anhang kann gesäubert werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang säubern** ausgewählt haben.
  - **Anhang verschieben**: Der infizierte Anhang kann verschoben werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang verschieben** ausgewählt haben.
  - **Anhang löschen**: Der infizierte Anhang kann gelöscht werden. Diese Option ist deaktiviert, wenn Sie als primäre Aktion **Anhang löschen** ausgewählt haben.

  Für diese Option ist keine sekundäre Aktion zulässig.

- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung eines infizierten Anhangs fortgesetzt.

  Für diese Option ist keine sekundäre Aktion zulässig.

- **Infizierte Anhänge in Ordner verschieben**: Infizierte Anhänge werden in einen Quarantäneordner verschoben. Der Standardname des Quarantäneordners lautet *Quarantine*. Sie können den Standardnamen des Ordners übernehmen oder einen neuen Namen eingeben.

  HINWEIS
  Der *Quarantäneordner* wird in der MAPI-Datenbank erstellt und kann in Microsoft Outlook in der **Ordnerliste** angezeigt werden.

- **Infizierte Anhänge säubern**: *Diese Option ist standardmäßig ausgewählt*. Der Scanner versucht, den Virus aus dem infizierten Anhang zu entfernen. Wenn der Scanner den Virus nicht aus einem infizierten Anhang entfernen kann oder der Virus den Anhang irreparabel beschädigt hat, führt der Scanner die sekundäre Aktion aus.

- **Infizierte Anhänge löschen**: Infizierte Anhänge werden bei Erkennung sofort gelöscht. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Anhänge erfasst werden.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

5 Wählen Sie unter **Wenn die oben genannte Aktion fehlschlägt** die sekundäre Aktion aus, die das Scan-Programm beim Fehlschlagen der primären Aktion ausführen soll.

> **HINWEIS**
> Bei der sekundären Standardaktion handelt es sich um **Infizierte Anhänge in Ordner verschieben**.

Klicken Sie auf  , um eine dieser Aktionen auszuwählen:

- **Aktion anfordern**: Bei Erkennung eines Virus wird eine Eingabeaufforderung an den Benutzer ausgegeben.

  Wenn diese Option ausgewählt wurde, können Sie festlegen, welche Aktionen neben Stoppen und Fortfahren noch zulässig sind. Folgende Optionen stehen zur Auswahl:

  - **Anhang säubern**: Der infizierte Anhang kann gesäubert werden.
  - **Anhang verschieben**: Der infizierte Anhang kann verschoben werden.
  - **Anhang löschen**: Der infizierte Anhang kann gelöscht werden.

- **Scan-Vorgang fortsetzen**: Der Scan-Vorgang wird bei Erkennung einer infizierten Datei fortgesetzt.

- **Infizierte Anhänge in Ordner verschieben**: *Diese Option ist standardmäßig ausgewählt.* Infizierte Anhänge werden in einen Quarantäneordner verschoben. Der Standardname des Quarantäneordners lautet *Quarantine*. Sie können den Standardnamen des Ordners übernehmen oder einen neuen Namen eingeben.

  > **HINWEIS**
  > Der *Quarantäneordner* wird in der MAPI-Datenbank erstellt und kann in Microsoft Outlook in der **Ordnerliste** angezeigt werden.

- **Infizierte Anhänge löschen**: Infizierte Anhänge werden bei Erkennung sofort gelöscht. Achten Sie darauf, dass die Eigenschaft **In Datei protokollieren** auf der Registerkarte **Berichte** aktiviert ist, damit die infizierten Anhänge erfasst werden.

  Bei Auswahl dieser Option müssen Sie die Auswahl bestätigen. Klicken Sie auf **Ja**, um Ihre Auswahl zu bestätigen, bzw. auf **Nein**, um diese Option zu deaktivieren.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Warnungseigenschaften

Wählen Sie die Optionen auf der Registerkarte **Warnungen**, um die Warnungen zu konfigurieren, die Benutzern bei Erkennung einer infizierten E-Mail-Nachricht bzw. eines Anhangs angezeigt werden.

1. Starten Sie Microsoft Outlook.
2. Rufen Sie das Dialogfeld **Eigenschaften des E-Mail-Scannens auf Anforderung** mit einer dieser Verfahrensweisen auf:
   - Wählen Sie aus dem Menü **Extras** die Option **E-Mail-Scan-Eigenschaften**.
   - Klicken Sie in der Symbolleiste von Outlook auf .

     HINWEIS
     Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard*-Symbolleiste auf und wählen dann das Symbol.
3. Wählen Sie die Registerkarte **Warnungen** aus.

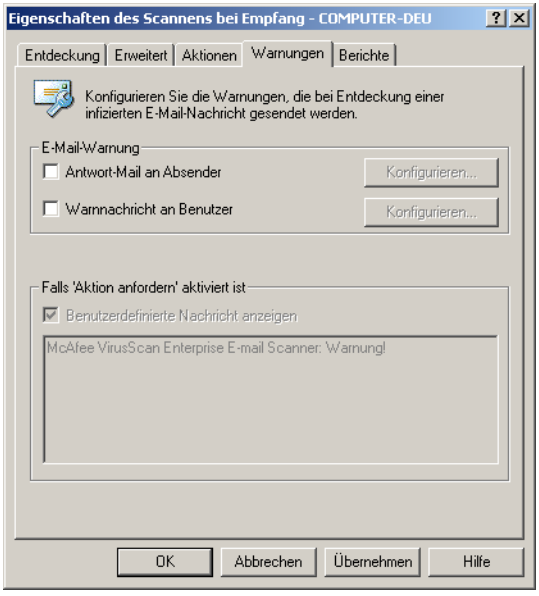


Abbildung 5-15. Eigenschaften des E-Mail-Scannens auf Anforderung – Registerkarte "Warnungen"

4 Geben Sie unter **E-Mail-Warnung** an, wie Absender und Benutzer von E-Mails bei Erkennung einer infizierten Nachricht benachrichtigt werden sollen. Sie haben folgende Optionen:

- **Antwort-Mail an Absender**: An den Absender wird eine Antwort-Mail gesendet.
  - Wenn Sie diese Option wählen, müssen Sie auf **Konfigurieren** klicken, um das Dialogfeld **"E-Mail zurücksenden" konfigurieren** aufzurufen.

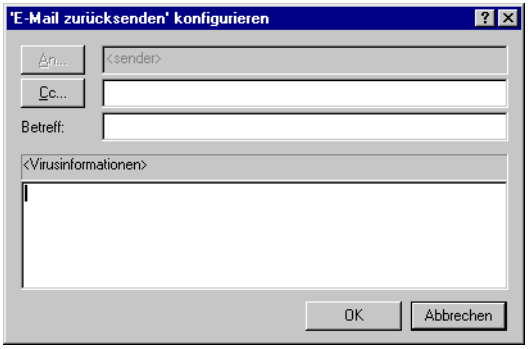


Abbildung 5-16. E-Mail-Scan – "E-Mail zurücksenden" konfigurieren

  - Geben Sie die Nachricht ein, die gesendet werden soll, und klicken Sie auf **OK**.

- **Warn-Mail an Benutzer senden**: Es wird eine Warn-E-Mail an einen Benutzer gesendet.
  - Wenn Sie diese Option gewählt haben, klicken Sie auf **Konfigurieren**, um das Dialogfeld **"E-Mail senden" konfigurieren** aufzurufen.

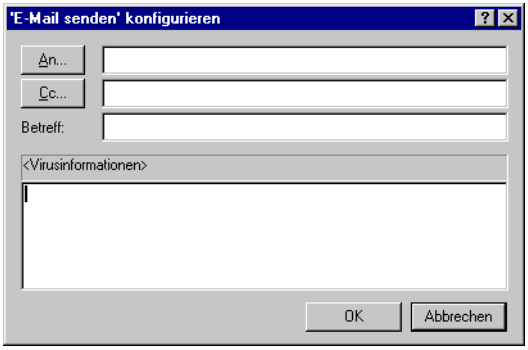


Abbildung 5-17. E-Mail-Scan – "E-Mail senden" konfigurieren

- Geben Sie die Nachricht ein, die gesendet werden soll, und klicken Sie auf **OK**.

5 Geben Sie unter **Falls "Aktion anfordern" aktiviert ist** an, wie die Benutzer bei Erkennung einer infizierten E-Mail benachrichtigt werden sollen. Sie haben folgende Optionen:

- **Benutzerdefinierte Nachricht anzeigen**: Der Benutzer erhält eine benutzerdefinierte Nachricht. Wenn Sie diese Option auswählen, können Sie eine benutzerdefinierte Nachricht in das Textfeld eingeben.
- **Akustische Warnung**: Der Benutzer wird durch ein akustisches Signal benachrichtigt.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Berichtseigenschaften

Klicken Sie auf die Registerkarte **Berichte**, um die Protokollierungsaktivitäten zu konfigurieren. Geben Sie den Speicherort und die Größe der Protokolldatei sowie die Informationen an, die Sie pro Protokolleintrag erfassen möchten.

HINWEIS
Die Protokolldatei ist ein wichtiges Verwaltungstool, mit dem Sie Virenaktivitäten in E-Mail-Nachrichten verfolgen und die vom Scanner zur Erkennung und Behandlung erkannter Viren verwendeten Einstellungen festhalten können. Die Protokolldatei kann später zur Prüfung im Texteditor geöffnet werden. Anhand der in der Datei protokollierten Ereignisse können Sie feststellen, welche Dateien durch Sicherungskopien ersetzt, im Quarantäneordner geprüft oder vom Rechner gelöscht werden müssen.

1 Starten Sie Microsoft Outlook.

2 Rufen Sie das Dialogfeld **Eigenschaften des E-Mail-Scannens auf Anforderung** mit einer dieser Verfahrensweisen auf:

- Wählen Sie aus dem Menü **Extras** die Option **E-Mail-Scan-Eigenschaften**.
- Klicken Sie in der Symbolleiste von Outlook auf  .

HINWEIS
Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard*-Symbolleiste auf  und wählen dann das Symbol.

3 Wählen Sie die Registerkarte **Berichte**.

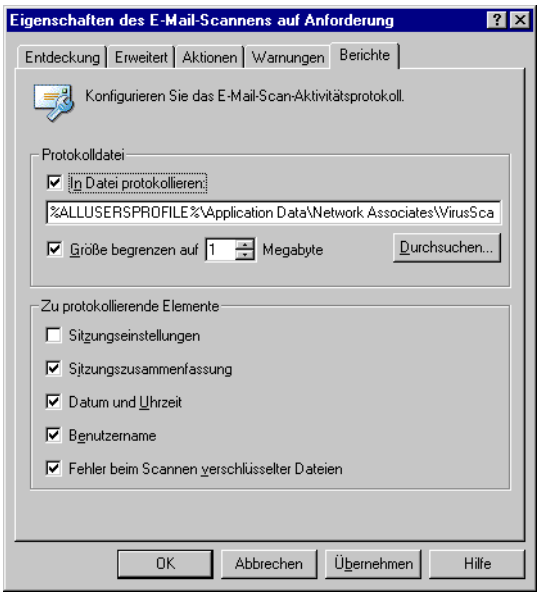


Abbildung 5-18. Eigenschaften des E-Mail-Scannens auf Anforderung – Registerkarte "Berichte"

4 Wählen Sie unter **Protokolldatei** eine dieser Optionen:

- **In Datei protokollieren**: *Diese Option ist standardmäßig ausgewählt.* Virusaktivitäten werden beim Scannen von E-Mails auf Anforderung in einer Protokolldatei aufgezeichnet.
- Sie können den im Textfeld angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einer anderen geeigneten Datei auf dem Computer oder im Netzwerk zu wechseln.

  HINWEIS
  Standardmäßig schreibt der Scanner Protokollinformationen in die Datei EMAILONDEMANDLOG.TXT in diesem Ordner:

  ```
  <Laufwerk>:Winnt\Profiles\All Users\Application
  Data\Network Associates\VirusScan
  ```

- **Größe begrenzen auf**: *Diese Option ist standardmäßig ausgewählt. Die Standardgröße der Protokolldatei ist 1 MB.* Übernehmen Sie die Standardgröße, oder legen Sie einen anderen Wert für die Protokolldatei fest. Wenn Sie diese Option auswählen, geben Sie einen Wert zwischen 1 MB und 999 MB ein.

HINWEIS
Wenn die Datenmenge in der Protokolldatei die von Ihnen festgelegte Dateigröße übersteigt, werden 20 Prozent der Protokolldateieinträge (die ältesten) gelöscht und der Datei neue Daten hinzugefügt.

5 Legen Sie unter **Zusätzlich zur Virusaktivität zu protokollierende Aktionen** fest, welche zusätzlichen Informationen in der Protokolldatei aufgezeichnet werden sollen:

- **Sitzungseinstellungen**: In der Protokolldatei werden die für die einzelnen Scan-Sitzungen ausgewählten Eigenschaften erfasst.
- **Sitzungszusammenfassung** *Diese Option ist standardmäßig ausgewählt.* Die Aktionen des Scanners bei den einzelnen Scan-Sitzungen werden zusammengefasst und derf Protokolldatei hinzugefügt. Zu den Zusammenfassungsinformationen gehören die Anzahl der gescannten Dateien, Anzahl und Typ der entdeckten Viren, die Anzahl der verschobenen, gelöschten oder bereinigten Dateien sowie weitere Informationen.
- **Datum und Uhrzeit**: *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden Datum und Uhrzeit der Erkennung eines Virus erfasst.
- **Benutzername** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei wird der Name des Benutzers erfasst, der zum Zeitpunkt der Aufzeichnung der jeweiligen Protokolleinträge auf dem Computer angemeldet war.
- **Fehler beim Scannen verschlüsselter Dateien** *Diese Option ist standardmäßig ausgewählt.* In der Protokolldatei werden die Namen der verschlüsselten Dateien erfasst, die nicht gescannt werden konnten.

6 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

Ausführen des E-Mail-Anforderungstasks

So führen Sie den E-Mail-Anforderungstask aus:

1 Starten Sie Microsoft Outlook.

2 Starten Sie einen E-Mail-Anforderungsscan aus Microsoft Outlook mit einem der folgenden Verfahren:

- Wählen Sie aus dem Menü **Extras** die Option **Nach Viren scannen**.
- Klicken Sie in der Symbolleiste von Outlook auf  .

HINWEIS

Wenn das Symbol in der Outlook-Symbolleiste nicht sichtbar ist, klicken Sie auf der rechten Seite der *Standard*-Symbolleiste auf  und wählen dann das Symbol.

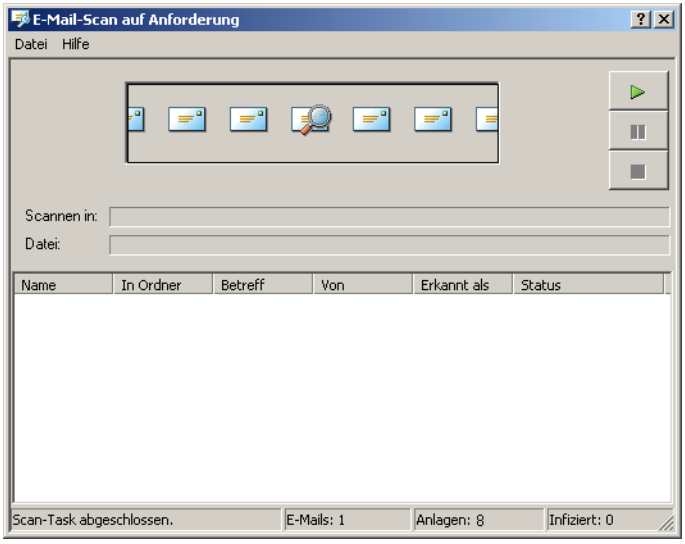


Abbildung 5-19. E-Mail-Scan auf Anforderung

3 Schließen Sie das Dialogfeld, wenn der E-Mail-Anforderungsscan abgeschlossen ist.

Anzeigen der Ergebnisse des E-Mail-Anforderungsscans

Sie können die Ergebnisse des Scan-Vorgangs während der Ausführung im Dialogfeld **E-Mail-Scan auf Anforderung** oder nach Abschluss des Scan-Vorgangs im Aktivitätsprotokoll anzeigen.

In diesem Abschnitt wird das folgende Thema behandelt:

- Anzeigen des Protokolls für E-Mail-Aktivitäten auf Anforderung

Anzeigen des Protokolls für E-Mail-Aktivitäten auf Anforderung

Das Aktivitätsprotokoll für das Scannen von E-Mail-Nachrichten auf Anforderung zeigt spezifische Details zum ausgeführten Scan-Vorgang an. So werden beispielsweise die Anzahl der vom Scanner überprüften Anhänge, die Anzahl der gefundenen Viren sowie die jeweils als Reaktion ausgeführten Aktionen angezeigt.

1. Navigieren Sie im folgenden Verzeichnis zu der Datei EMAILONDEMANDLOG.TXT:

   ```
   <Laufwerk>:Winnt\Profiles\All Users\Application Data\Network
   Associates\VirusScan
   ```

2. Öffnen Sie die Aktivitätsprotokolldatei.
3. Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

Virenwarnungen 6

Die Software VirusScan Enterprise bietet Ihnen verschiedene Möglichkeiten, Informationen zum Status und zu den Ergebnissen der Scan-Aktivitäten abzurufen. So können Sie die Ergebnisse eines Scan-Vorgangs beispielsweise nach Abschluss des entsprechenden Vorgangs im Aktivitätsprotokoll prüfen. Außerdem werden in der VirusScan Enterprise-Konsole die Ergebnisse aller Scan-Vorgänge angezeigt. Eine sofortige Benachrichtigung bei Entdeckung eines Virus auf dem Computer erhalten Sie mit diesen beiden Methoden jedoch nicht. Die Konsole enthält zwar auch eine Echtzeitanzeige der Scan-Aktivitäten, aber Sie werden kaum in der Lage sein, den Bildschirm ununterbrochen zu überwachen. Die Ausgabe von Benachrichtigungen bei der Erkennung eines Virus ist die Aufgabe des Warnungs-Managers. Dabei handelt es sich um eine separate Komponente, die in der Software VirusScan Enterprise und anderen Client-/Server-Sicherheits- und -verwaltungslösungen von Network Associates enthalten ist.

Der Warnungs-Manager bearbeitet die durch Ihre Virenschutz-Software erzeugten Warnungen und Ereignisse in Echtzeit. Bei einer Standardkonfiguration befindet sich der Warnungs-Manager auf einem zentralen Server. Er überwacht das Netzwerk auf Warnungen durch Virenschutz-Software-Anwendungen auf einem Client oder einem Server. Die Client-Software kann eine Anwendung auf einer Arbeitsstation oder auf einem Server sein. Sie können mit dem Warnungs-Manager zwei grundlegende Funktionen konfigurieren:

- Wohin und wie werden Warnungen gesendet.
- Worin besteht die Warnmeldung.

Weitere Informationen finden Sie im *Warnungs-Manager-Produkthandbuch*.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Konfigurieren des Warnungs-Managers
- Konfigurieren von Empfängern und Methoden
- Anpassen von Warnmeldungen

Konfigurieren des Warnungs-Managers

Verwenden Sie die Optionen im Dialogfeld **Warnungseigenschaften**, um anzugeben, wann und wie oft Sie benachrichtigt werden möchten, wenn der Scanner einen Virus findet.

So rufen Sie das Dialogfeld **Warnungseigenschaften** auf:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

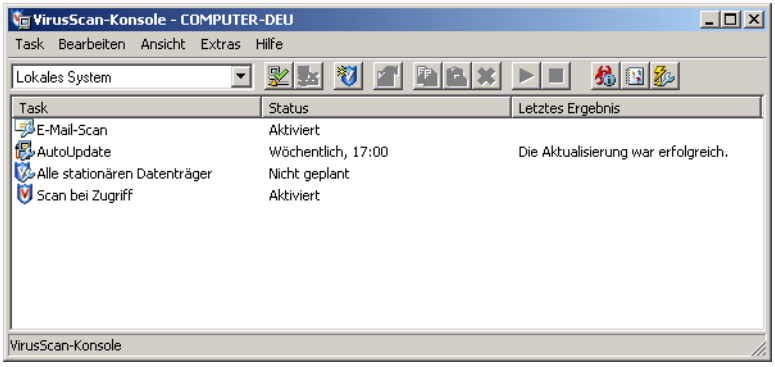


Abbildung 6-1. VirusScan-Konsole

2 Wählen Sie aus dem Menü **Extras** die Option **Warnungen**.

Das Dialogfeld **Warnungseigenschaften** wird angezeigt.

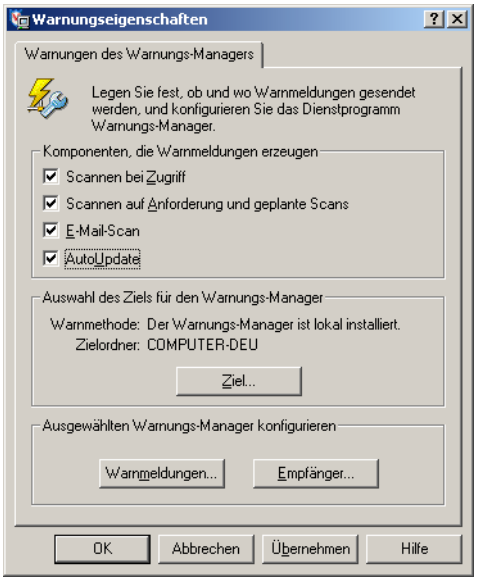


Abbildung 6-2. Warnungseigenschaften

3 Wählen Sie unter **Komponenten, die Warnmeldungen erzeugen** die Komponenten aus, die mit dem Warnungs-Manager kommunizieren sollen. Wählen Sie eine beliebige Kombination der folgenden Optionen:

- **Scannen bei Zugriff**: *Diese Option ist standardmäßig ausgewählt.*
- **Scannen auf Anforderung und geplante Scans**: *Die Option ist standardmäßig ausgewählt.*
- **E-Mail-Scan**: *Die Option ist standardmäßig ausgewählt.*
- **AutoUpdate**: *Die Option ist standardmäßig ausgewählt.*

4 Klicken Sie unter **Auswahl des Zieles für den Warnungs-Manager** auf **Ziel**, um das Dialogfeld **Warnungs-Manager - Client-Konfiguration** zu öffnen.

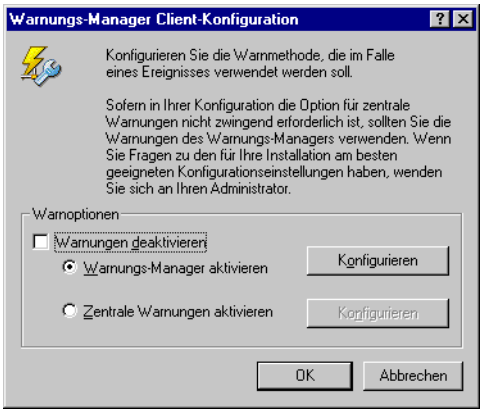

Warnungs-Manager Client-Konfiguration
Konfigurieren Sie die Warnmethode, die im Falle eines Ereignisses verwendet werden soll.
Sofern in Ihrer Konfiguration die Option für zentrale Warnungen nicht zwingend erforderlich ist, sollten Sie die Warnungen des Warnungs-Managers verwenden. Wenn Sie Fragen zu den für Ihre Installation am besten geeigneten Konfigurationseinstellungen haben, wenden Sie sich an Ihren Administrator.
Warnoptionen
Warnungen deaktivieren
Warnungs-Manager aktivieren
Konfigurieren
Zentrale Warnungen aktivieren
Konfigurieren
OK
Abbrechen

Abbildung 6-3. Warnungs-Manager – Client-Konfiguration

Sie können die Warnfunktion aktivieren oder deaktivieren, die Warnmethode bei einem Ereignis sowie den Server festlegen, der die Warnungen empfängt.

a Geben Sie unter **Warnoptionen** die Warnmethode an, die Ihren Anforderungen am besten entspricht:.

- **Warnungen deaktivieren**: Bei einem Ereignis soll keine Warnung gesendet werden.
- **Warnungs-Manager aktivieren**: *Diese Option ist standardmäßig ausgewählt.* Die Warnmethode des Warnungs-Managers wird aktiviert.

  Konfigurieren : Wenn die Option **Warnungs-Manager aktivieren** aktiviert wurde, klicken Sie auf **Konfigurieren**, um das Dialogfeld **Warnungs-Manager-Server auswählen** zu öffnen.

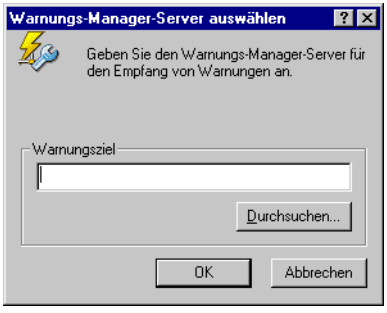


Abbildung 6-4. Warnungs-Manager-Server auswählen

Geben Sie unter **Warnungsziel** den Pfad für den **Warnungs-Manager-Server** ein, der die Warnungen erhalten soll, oder klicken Sie auf **Durchsuchen**, um zum entsprechenden Verzeichnis zu wechseln.

Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Warnungs-Manager Client-Konfiguration** zurückzukehren.

- **Zentrale Warnungen aktivieren**: Die zentrale Warnmethode wird aktiviert. Zentrale Warnungen stellen eine Alternative zur regulären Verwendung des Warnungs-Managers beim Versenden von Meldungen dar. Weitere Informationen finden Sie unter *Verwenden von zentralen Warnungen* auf Seite 190.

  HINWEIS
  Auf Grund der Sicherheitsprobleme, die bei freigegebenen Ordnern entstehen können, empfiehlt McAfee Security, die Funktion "Zentrale Warnungen" möglichst *nicht* einzusetzen.

  Konfigurieren : Wenn die Option **Zentrale Warnungen aktivieren** aktiviert wurde, klicken Sie auf **Konfigurieren**, um das Dialogfeld **Zentrale Warnungen konfigurieren** zu öffnen.

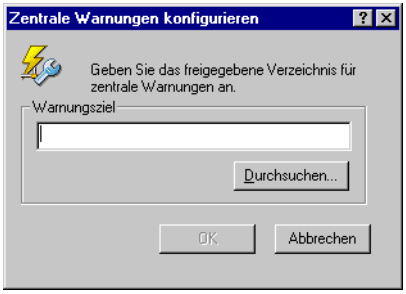


Abbildung 6-5. Konfiguration zentraler Warnungen

Geben Sie unter **Warnungsziel** den Pfad für das **Freigegebene Verzeichnis für zentrale Warnungen** ein, oder klicken Sie auf **Durchsuchen**, um zum entsprechenden Verzeichnis zu wechseln.

Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Warnungs-Manager Client-Konfiguration** zurückzukehren.

b Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Warnungseigenschaften** zurückzukehren.

5 Rufen Sie zunächst **Ausgewählten Warnungs-Manager konfigurieren** auf.

a Klicken Sie auf **Warnmeldungen**, um die **Warnungs-Manager-Nachrichten** zu konfigurieren. Ausführliche Anweisungen dazu finden Sie unter *Anpassen von Warnmeldungen* auf Seite 192.

HINWEIS
Die Schaltfläche **Warnmeldungen** ist deaktiviert, wenn der Warnungs-Manager nicht installiert ist.

b Klicken Sie auf **Empfänger**, um die **Eigenschaften des Warnungs-Managers** zu konfigurieren. Ausführliche Anweisungen dazu finden Sie unter *Konfigurieren von Empfängern und Methoden* auf Seite 166.

HINWEIS
Die Schaltfläche **Empfänger** ist deaktiviert, wenn der Warnungs-Manager nicht installiert ist.

c Klicken Sie auf **Warnmeldungen**, um die **Warnungs-Manager-Nachrichten** zu konfigurieren. Ausführliche Anweisungen dazu finden Sie unter *Anpassen von Warnmeldungen* auf Seite 192.

HINWEIS
Die Schaltfläche **Warnmeldungen** ist deaktiviert, wenn der Warnungs-Manager nicht installiert ist.

d Wenn Sie die Konfiguration der **Eigenschaften des Warnungs-Managers** und der **Warnungs-Manager-Nachrichten** abgeschlossen haben, klicken Sie auf **OK**, um das Dialogfeld **Warnungseigenschaften** zu schließen.

Konfigurieren von Empfängern und Methoden

Klicken Sie im Dialogfeld **Warnungseigenschaften** auf **Empfänger**, um das Dialogfeld **Eigenschaften des Warnungs-Managers** aufzurufen.

Im Dialogfeld **Eigenschaften des Warnungs-Managers** können die *Empfänger* der durch den Warnungs-Manager gesendeten Warnmeldungen konfiguriert werden. Außerdem wird hier unter *Methode* festgelegt, auf welche Weise diese Empfänger die Warnmeldungen erhalten. Empfänger können E-Mail-Adressen oder Computer in Ihrem Netzwerk sein. Zu den Methoden, die bei der Verteilung der Warnbenachrichtigungen an die Empfänger eingesetzt werden, gehören E-Mails und Popup-Netzwerkmeldungen.

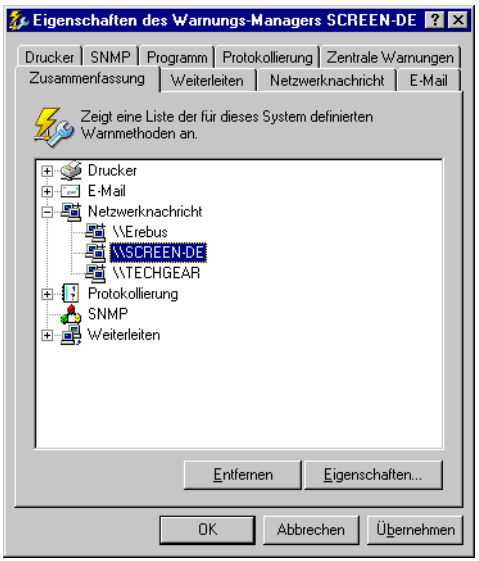


Abbildung 6-6. Eigenschaften des Warnungs-Managers

So konfigurieren Sie die Empfänger für eine bestimmte Warnmethode:

1. Klicken Sie auf die Registerkarte für die betreffende Warnmethode, z. B. **Protokollierung**.
2. Konfigurieren Sie die Empfänger, denen mit dieser Warnmethode Warnbenachrichtigungen zugestellt werden sollen.
3. Klicken Sie auf eine andere Registerkarte, wenn Empfänger für weitere Warnmethoden konfiguriert werden sollen.
4. Wenn Sie fertig sind, klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Eigenschaften des Warnungs-Managers** zu schließen.

Einzelheiten zur Konfiguration der Warnmethoden und Empfänger, an die der Warnungs-Manager die Warnmeldungen mithilfe der ausgewählten Methoden sendet, finden Sie in den entsprechenden Abschnitten dieser :

- *Anzeigen der Seite "Zusammenfassung"* auf Seite 170
- *Weiterleiten von Warnmeldungen an andere Computer* auf Seite 171
- *Senden von Warnungen als Netzwerkmeldungen* auf Seite 175
- *Senden von Warnmeldungen an E-Mail-Adressen* auf Seite 177
- *Senden von Warnmeldungen an einen Drucker* auf Seite 181
- *Senden von Warnmeldungen per SNMP* auf Seite 183

- *Starten eines Programms als Warnung* auf Seite 185
- *Protokollieren von Warnbenachrichtigungen im Ereignisprotokoll des Computers* auf Seite 186
- *Senden einer Netzwerkmeldung an einen Terminalserver* auf Seite 188. Diese Methode ist nur verfügbar, wenn auf dem Computer, auf dem der Warnungs-Manager installiert ist, Terminaldienste ausgeführt werden.
- *Verwenden von zentralen Warnungen* auf Seite 190

Überblick über das Hinzufügen von Warnmethoden

Mithilfe der verschiedenen Registerkarten im Dialogfeld **Eigenschaften des Warnungs-Managers** können Warnmethoden konfiguriert werden. Beim Hinzufügen der einzelnen neuen Methoden zur Konfiguration stehen Ihnen zwei Optionen zur Verfügung:

- Senden einer Testnachricht.
- Einrichten der Warnungsprioritätsstufe für Empfänger.

Senden einer Testnachricht

Wenn Sie zum Hinzufügen neuer Empfänger für Warnbenachrichtigungen, z. B. eines Netzwerkcomputers oder einer E-Mail-Adresse, die Registerkarten des Dialogfelds **Eigenschaften des Warnungs-Managers** verwenden, können Sie testen, ob das Ziel die Nachricht empfangen kann. Um beim Konfigurieren der Methode eine Testnachricht an das ausgewählte Ziel zu senden, klicken Sie auf die Schaltfläche **Test**.

Wenn die Konfiguration fehlerfrei ist, wird die Nachricht am angegebenen Ziel angezeigt.

> **HINWEIS**
> Die bis zum Eintreffen der E-Mail-Warnung am Bestimmungsort verstreichende Zeit ist von Ihrem SMTP-Server und dem E-Mail-Server abhängig, der die Mail empfängt.

Testnachrichten, die das Ziel nicht erreichen

Wenn die Nachricht nicht vom Ziel empfangen wird, überprüfen und bestätigen Sie ggf. die in der Liste angegebenen Punkte:

- Die für die Implementierung der ausgewählten Warnmethode erforderlichen Kommunikationsdienste, z. B. E-Mail oder SNMP, sind aktiviert.
- Die zur Übertragung oder zum Empfang der Nachricht erforderlichen Geräte, z. B. Modem oder Pager, sind vorhanden und betriebsbereit.

- Die als Antwort auf die Virenerkennung auszuführenden Programme sind geladen, sie wurden im angegebenen Verzeichnis abgelegt und ordnungsgemäß installiert.
- Die als Ziel angegebenen Drucker oder Computer sind im Netzwerk vorhanden.
- Das Netzwerk funktioniert ordnungsgemäß.
- Die zur Verfügung gestellten Konfigurationsinformationen sind vollständig und genau. Einige Eigenschaftenseiten haben eine zweite Seite. Die Seite mit den **E-Mail-Eigenschaften** ist beispielsweise mit einer Seite für E-Mail-Einstellungen verknüpft. Achten Sie darauf, dass auch die Informationen auf den dazugehörigen zweiten Seiten geprüft werden.
- Wenn Sie den Warnungs-Manager unter Verwendung eines Kontos und eines Kennworts installiert haben, sollten Sie sich vergewissern, dass das angegebene Konto über die für die Aktion erforderlichen Zugriffsrechte verfügt.

Einrichten der Warnungsprioritätsstufe für Empfänger

Sie können für jeden Empfänger, den Sie Ihrer Warnungs-Manager-Konfiguration hinzufügen, eine Prioritätsstufe angeben. An den jeweiligen Empfänger, z. B. eine E-Mail-Adresse, sendet der Warnungs-Manager dann nur noch Warnbenachrichtigungen dieser oder einer höheren Prioritätsstufe.

Damit kann die Einstellung vor allem zum Filtern von Warnbenachrichtigungen sinnvoll eingesetzt werden. Beispiel: Im Ereignisprotokoll eines Computers sollen über die Registerkarte **Protokollierung** im Dialogfeld **Eigenschaften des Warnungs-Managers** (siehe *Protokollieren von Warnbenachrichtigungen im Ereignisprotokoll des Computers* auf Seite 186) Warnmeldungen aller Prioritätsstufen erfasst werden. Der Warnungs-Manager soll jedoch nur die wichtigen Warnbenachrichtigungen per E-Mail an den Pager des Netzwerk-Administrators senden. Dazu richten Sie für Protokoll- und E-Mail-Empfänger verschiedene Prioritätsschwellen ein.

So richten Sie die Warnungsprioritätsstufe für einen Empfänger ein:

1 Klicken Sie im Dialogfeld **Eigenschaften** einer Warnmethode auf die Schaltfläche **Prioritätsstufe**.

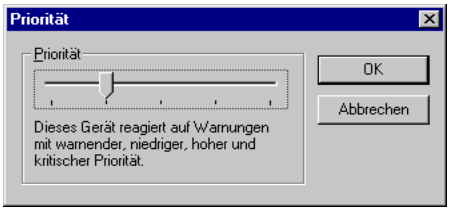


Abbildung 6-7. Prioritätsstufe

2 Ziehen Sie den Regler im Dialogfeld **Prioritätsstufe** nach rechts oder links, um die Prioritätsstufe einzustellen.

Wenn der Empfänger weniger Nachrichten mit einer höheren Priorität erhalten soll, ziehen Sie den Regler nach rechts. Ziehen Sie den Regler nach links, um mehr Warnmeldungen, einschließlich der Meldungen mit niedriger Priorität, an den Empfänger zu senden.

3 Klicken Sie auf **OK**, um die Prioritätseinstellungen zu speichern.

HINWEIS
Im Dialogfeld **Prioritätsstufe** kann die Prioritätsstufe für bestimmte Empfänger, z. B. einen Netzwerkcomputer oder eine E-Mail-Adresse, angegeben werden. Die Priorität einzelner Warnmeldungen kann hier jedoch *nicht* eingestellt werden. Informationen zur Einrichtung der Prioritätsstufen für einzelne Warnmeldungen finden Sie unter *Anpassen von Warnmeldungen* auf Seite 192.

Anzeigen der Seite "Zusammenfassung"

Im Dialogfeld **Eigenschaften des Warnungs-Managers** werden auf der Registerkarte **Zusammenfassung** die Empfänger aufgelistet, an die der Warnungs-Manager die erhaltenen Warnbenachrichtigungen sendet. Die Empfänger sind nach Warnmethoden in Gruppen geordnet.

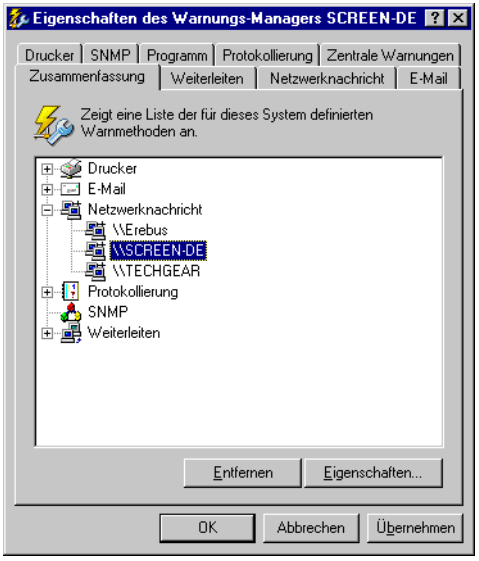


Abbildung 6-8. Eigenschaften des Warnungs-Managers – Registerkarte "Zusammenfassung"

Klicken Sie in der Liste neben jeder aufgelisteten Warnmethode auf ⊞, um die Computer, Drucker, bzw. E-Mail-Adressen anzuzeigen, die als Empfänger angegeben wurden. Um einen Empfänger der Warnbenachrichtigung zu entfernen, wählen Sie ihn aus, und klicken Sie anschließend auf **Entfernen.** Um die Konfigurationsoptionen für einen Empfänger in der Liste zu ändern, wählen Sie ihn aus, und klicken Sie dann auf **Eigenschaften**, um das Dialogfeld **Eigenschaften** für die Warnmethode aufzurufen.

Wenn Sie den Warnungs-Manager installieren, ist er standardmäßig so konfiguriert, dass Popup-Netzwerkmeldungen an den Computer gesendet werden, auf dem der Warnungs-Manager installiert ist. Die Warnbenachrichtigungen werden dann im Ereignisprotokoll dieses Computers erfasst. Wenn der Warnungs-Manager noch nicht für das Senden von Warnbenachrichtigungen an Empfänger konfiguriert wurde, werden auf der Registerkarte **Zusammenfassung** nur diese beiden Methoden angezeigt. Der Warnungs-Manager stellt die Prioritätsstufen für diese beiden Standardmethoden so ein, dass mit Ausnahme der niedrigsten Prioritätsstufe, **Information**, Warnbenachrichtigungen aller Prioritätsstufen gesendet werden. Genauere Informationen zur Priorität finden Sie unter *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

In den folgenden Abschnitten werden die für die einzelnen Methoden verfügbaren Optionen erläutert.

Weiterleiten von Warnmeldungen an andere Computer

Der Warnungs-Manager kann die von McAfee Client- oder Server-Virenschutzprodukten empfangenen Warnmeldungen an einen anderen Netzwerkcomputer weiterleiten, auf dem der Warnungs-Manager installiert ist. Diese Option wird in der Regel ausgeführt, wenn Meldungen zur weiteren Verteilung an einen anderen Warnungs-Manager-Server weitergeleitet werden sollen.

HINWEIS
Der Warnungs-Manager 4.7 kann Warnmeldungen nur an Server weiterleiten bzw. von Servern empfangen, die dieselbe Version des Warnungs-Managers ausführen. Die Weiterleitung von Warnmeldungen zwischen Servern mit älteren Versionen des Warnungs-Managers wird nicht unterstützt.

Weiterleiten von Warnungen in großen Unternehmen

In großen Unternehmen kann die Weiterleitungsfunktion dazu eingesetzt werden, Warnbenachrichtigungen zur Verfolgung der Virenstatistik und der Problembereiche an ein zentrales Benachrichtigungssystem oder an die MIS-Abteilung (Management Information System) zu senden. Größere Unternehmen sind häufig international tätig und haben daher Niederlassungen in verschiedenen Ländern. In einem solchen Fall sollten Sie eine einzelne Warnungs-Manager-Installation auf einem lokalen Server verwenden, um die Warnungen für dieses lokale Unternetzwerk zu verarbeiten. Sie können dann diesen lokalen Warnungs-Manager-Server so konfigurieren, dass Warnungen mit hoher Priorität an einen anderen Server in einem anderen Bereich Ihres Netzwerks zur Verteilung gesendet werden.

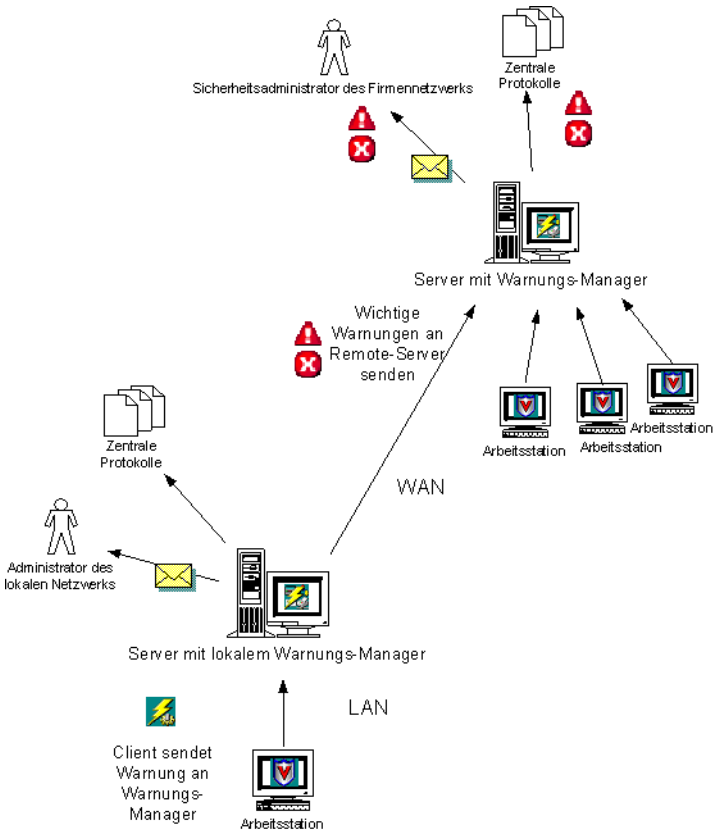


Abbildung 6-9. Warnungen an einen anderen Warnungs-Manager weiterleiten

Konfigurieren Sie dazu den lokalen Warnungs-Manager so, dass Warnungen an den Computer mit dem zweiten Warnungs-Manager weitergeleitet werden. Anschließend müssen Sie den zweiten Warnungs-Manager so konfigurieren, dass die Warnmeldungen wie gewünscht verteilt werden. Anweisungen dazu finden Sie unter *Konfigurieren von Optionen zum Weiterleiten von Warnungen* auf Seite 173.

Weiterleiten von Warnungen in kleinen Unternehmen

Die Weiterleitungsfunktion kann jedoch auch in kleineren Unternehmen sinnvoll eingesetzt werden. Beispiel: Sie möchten alle erzeugten Warnmeldungen mit hoher Priorität per E-Mail an einen bestimmten Pager senden. In Ihrem Netzwerk verfügt jedoch nur ein Server über einen direkten Internetzugang.

Um diese Aufgabe auszuführen, gehen Sie folgendermaßen vor:

1. Konfigurieren Sie den Warnungs-Manager auf allen Warnungs-Manager-Servern, um Warnmeldungen mit hoher Priorität an den mit Modem ausgestatteten Computer weiterzuleiten.
2. Konfigurieren Sie den Warnungs-Manager auf dem mit einem Modem ausgestatteten Computer, um Meldungen mit hoher Priorität an die E-Mail-Adresse des Ziel-Pagers zu senden.

Konfigurieren von Optionen zum Weiterleiten von Warnungen

So konfigurieren Sie die Weiterleitungsoptionen:

1. Klicken Sie im Dialogfeld **Eigenschaften des Warnungs-Managers** auf die Registerkarte **Weiterleiten**.

   Die Seite **Weiterleiten** wird angezeigt. Sie enthält eine Liste der Computer, die für den Empfang weitergeleiteter Meldungen ausgewählt wurden. Wenn noch keine Empfängercomputer ausgewählt wurden, enthält die Liste keine Einträge.



Abbildung 6-10. Eigenschaften des Warnungs-Managers – Registerkarte "Weiterleiten"

2 Um die Liste zu aktualisieren, können Sie folgendermaßen vorgehen:

- Wenn Sie einen Computer hinzufügen möchten, klicken Sie auf **Hinzufügen**, um das Dialogfeld **Weiterleitungseigenschaften** aufzurufen, und geben Sie in das Textfeld den Namen des Computers ein, der die weitergeleiteten Meldungen empfangen soll. Der Computername kann in UNC-Schreibweise (Universal Naming Convention) eingegeben werden, oder Sie klicken auf **Durchsuchen**, um den Computer im Netzwerk zu suchen.
- Um einen Computer aus der Liste zu entfernen, wählen Sie einen der aufgelisteten Empfängercomputer, und klicken Sie auf **Entfernen**.
- Um die Konfigurationsoptionen zu ändern, wählen Sie einen der aufgelisteten Empfängercomputer, und klicken Sie auf **Eigenschaften.** Der Warnungs-Manager ruft das Dialogfeld **Weiterleitungseigenschaften** auf. Geben Sie den Namen des Computers ein, an den der Warnungs-Manager die Meldungen weiterleiten soll, oder klicken Sie auf **Durchsuchen**, um den Computer im Netzwerk zu suchen.



Abbildung 6-11. Weiterleitungseigenschaften

3 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

4 Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

5 Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Senden von Warnungen als Netzwerkmeldungen

Der Warnungs-Manager kann Warnmeldungen an andere Computer senden. Standardmeldungen werden auf dem Bildschirm des Empfängercomputers als Popup-Text angezeigt und müssen vom Empfänger bestätigt werden.

Auf den Empfängercomputern muss der Warnungs-Manager nicht installiert sein. Auf dem Empfängercomputer muss jedoch möglicherweise die entsprechende Messaging-Client-Software für das verwendete Betriebssystem installiert sein. Diese Messaging-Software ist auf neueren Versionen des Windows-Betriebssystems, wie z. B. Windows NT, Windows 2000 und Windows XP, immer vorinstalliert. Dieser Dienst wird in der Regel standardmäßig ausgeführt.

So konfigurieren Sie den Warnungs-Manager, um Warnbenachrichtigungen als Netzwerkmeldungen zu senden:

1 Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.

2 Klicken Sie auf die Registerkarte **Netzwerkmeldung**. Die Seite **Netzwerkmeldung** wird angezeigt. Sie enthält eine Liste der Computer, die für den Empfang von Netzwerkmeldungen konfiguriert wurden. Wenn noch kein Empfängercomputer ausgewählt wurde, enthält die Liste keine Einträge.

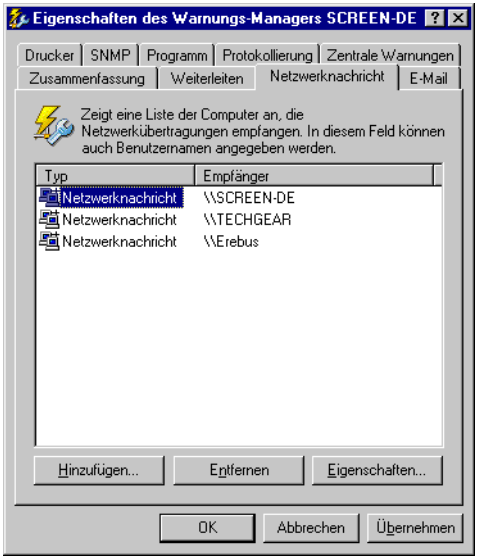


Abbildung 6-12. Eigenschaften des Warnungs-Managers – Registerkarte "Netzwerkmeldung"

3 Um die Liste zu aktualisieren, können Sie folgendermaßen vorgehen:

- Um einen Computer hinzuzufügen, klicken Sie auf **Hinzufügen**. Dadurch wird das Dialogfeld **Eigenschaften von Netzwerkmeldungen** angezeigt. Der Empfängercomputer kann auf zwei verschiedene Arten festgelegt werden. Sie können den Namen des Computers im UNC-Format direkt in das Textfeld **Computer:** eingeben, oder Sie klicken auf **Durchsuchen**, um den Computer im Netzwerk zu suchen.
- Um einen Computer aus der Liste zu entfernen, wählen Sie einen der aufgelisteten Empfängercomputer aus, und klicken Sie auf **Entfernen**.
- Um die Konfigurationsoptionen zu ändern, wählen Sie einen der aufgelisteten Empfängernamen aus, und klicken Sie auf **Eigenschaften.** Der Warnungs-Manager ruft das Dialogfeld **Eigenschaften von Netzwerkmeldungen** auf. Ändern Sie die Informationen im Textfeld **Computer:** nach Bedarf.



Abbildung 6-13. Eigenschaften von Netzwerkmeldungen

4 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfänger erhalten soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

5 Klicken Sie auf **Test**, um eine Testnachricht an den Empfänger zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

6 Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Senden von Warnmeldungen an E-Mail-Adressen

Der Warnungs-Manager kann Warnmeldungen per SMTP (Simple Mail Transfer Protocol) an die E-Mail-Adresse eines Empfängers senden. Warnmeldungen werden in der Mailbox des Empfängers angezeigt. Wenn es sich um eine besonders dringende Meldung handelt, können Sie die E-Mail durch andere Methoden, z. B. Popup-Netzwerkmeldungen, ergänzen. Auf diese Weise können Sie sicherstellen, dass der Empfänger die Warnung rechtzeitig bemerkt, um die entsprechenden Schritte zu unternehmen.

HINWEIS
Die bis zum Eintreffen der E-Mail-Warnung am Bestimmungsort verstreichende Zeit ist von Ihrem SMTP-Server und dem E-Mail-Server abhängig, der die Mail empfängt.

So konfigurieren Sie den Warnungs-Manager, um E-Mail-Warnbenachrichtigungen an Empfänger zu senden:

1 Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.

2 Klicken Sie auf die Registerkarte **E-Mail**.

Die Seite **E-Mail** wird angezeigt. Sie enthält eine Liste der E-Mail-Adressen, die für den Empfang von Warnmeldungen ausgewählt wurden. Wenn noch keine E-Mail-Adressen ausgewählt wurden, enthält die Liste keine Einträge.

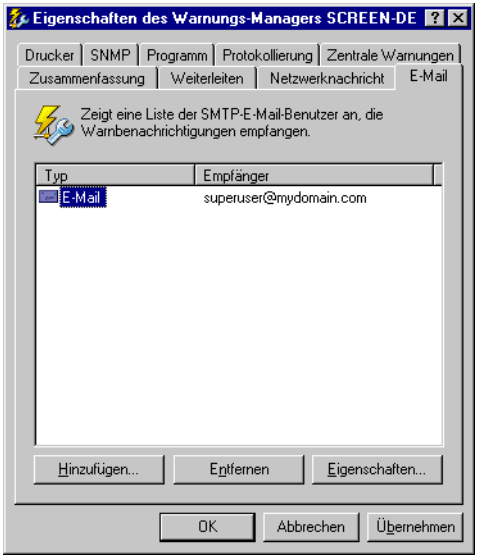


Abbildung 6-14. Eigenschaften des Warnungs-Managers – Registerkarte "E-Mail"

3 Um die Liste zu aktualisieren, können Sie folgendermaßen vorgehen:

- Um der Liste eine E-Mail-Adresse hinzuzufügen, klicken Sie auf **Hinzufügen**. Dadurch wird das Dialogfeld **Eigenschaften von E-Mail** aufgerufen. Geben Sie die E-Mail-Adresse des Empfängers der Warnbenachrichtigungen im Textfeld **Adresse** ein, geben Sie im Textfeld **Betreff** einen Betreff ein, und geben Sie anschließend im Textfeld **Von** Ihre E-Mail-Adresse ein. Verwenden Sie das Standardformat für Internetadressen `<benutzername>@<domäne>`, z. B. `administrator_1@mail.com`.

  Um zu verhindern, dass lange Meldungen abgeschnitten werden (z. B. eine Meldung mit sehr langem Datei- und Pfadnamen), hängen Sie an die Adresse wie folgt ein Sternchen (*) an: `administrator_1@mail.com*`. Weitere Informationen finden Sie unter *Erzwingen von abgeschnittenen Meldungen bei bestimmten E-Mail-Adressen* auf Seite 181.

- Um eine Adresse aus der Liste zu entfernen, wählen Sie eine aufgelistete E-Mail-Adresse aus, und klicken Sie auf **Entfernen**.
- Um die Konfigurationsoptionen zu ändern, wählen Sie eine der aufgelisteten E-Mail-Adressen aus, und klicken Sie auf **Eigenschaften.** Der Warnungs-Manager ruft das Dialogfeld **Eigenschaften von E-Mail** auf. Ändern Sie die Informationen im Textfeld nach Bedarf.



Abbildung 6-15. E-Mail-Eigenschaften

4 Klicken Sie auf **Mail-Einstellungen**, um den Netzwerkserver anzugeben, mit dem die Internet-Mails per SMTP gesendet werden soll.

HINWEIS
Um E-Mail-Warnbenachrichtigungen senden zu können, *müssen* Sie auf **Mail-Einstellungen** klicken und einen SMTP-Server angeben. Dieser Schritt darf keinesfalls ausgelassen werden. Sobald die SMTP-Mail-Einstellungen konfiguriert wurden, werden Sie nicht mehr aufgefordert, diese erneut zu konfigurieren, es sei denn, die SMTP-Mail-Serverdaten ändern sich.

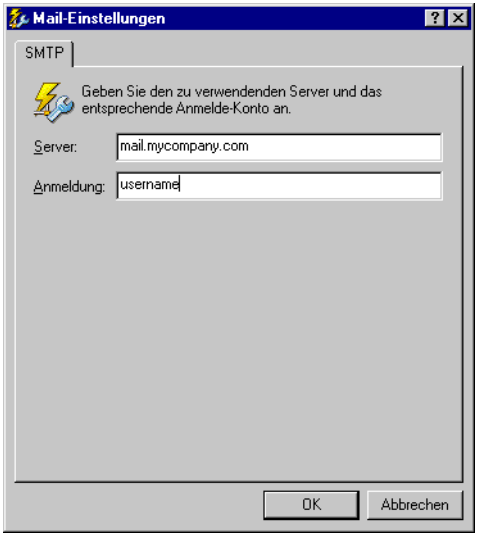


Abbildung 6-16. SMTP-Mail-Einstellungen

a Geben Sie im angezeigten Dialogfeld den **Mail-Server** ein. Der Servername kann in Form einer IP-Adresse (Internet Protocol), als Name, der vom lokalen DNS erkannt wird, oder im UNC-Format (Universal Naming Convention) eingegeben werden.

b Sofern dies bei Ihrem SMTP-Server erforderlich ist, geben Sie für den Mail-Server auch einen **Anmeldenamen** ein.

> **HINWEIS**
> Geben Sie im Feld **Anmeldung** nur dann einen Anmeldenamen ein, wenn Ihr SMTP-Mail-Server für die Verwendung von Anmeldedaten konfiguriert wurde. Prüfen Sie Ihre SMTP-Konfiguration, um festzustellen, ob dies erforderlich ist. Wenn Sie hier einen Anmeldenamen eingeben, obwohl Ihr Mail-Server nicht dafür konfiguriert wurde, kann dies zu Problemen beim Versenden von Warnungen per E-Mail führen.

c Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften von E-Mail** zurückzukehren.

5 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

6 Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

7 Wenn die Testnachricht erfolgreich ist, klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Erzwingen von abgeschnittenen Meldungen bei bestimmten E-Mail-Adressen

Manche Warnmeldungen sind sehr lang, insbesondere dann, wenn Sie `%FILENAME%`-Systemvariablen enthalten, die mit sehr langen Dateipfaden und -namen versehen sind. Sehr lange Meldungen mit langen Dateinamen können verwirrend und unübersichtlich sein. Per E-Mail an einen Pager gesendete lange Meldungen werden beispielsweise von einigen Pager-Diensten sofort abgeschnitten, wodurch unter Umständen wichtige Informationen entfernt werden. Wenn eine sehr lange Meldung einen Pager erreicht, muss der Empfänger den Dateipfad möglicherweise durchsuchen, um die wichtigen Informationen der Warnung zu erhalten.

Es stehen zwei Optionen für die Verwaltung von langen Meldungen in E-Mail-Warnbenachrichtigungen zur Verfügung:

- An E-Mail-Adressen wird ein Sternchen (*) angehängt, wie z. B. `administrator_1@mail.com*`. Der Warnungs-Manager schneidet Warnungen an mit einem Sternchen versehene E-Mail-Adressen gemäß den aktuellen SMTP-Längeneinstellungen ab. Die standardmäßige SMTP-Länge beträgt 240 Zeichen.

  Dies kann besonders sinnvoll sein, wenn der Warnungs-Manager Warnungen per E-Mail an Pager sendet. Einige Pager-Dienste verfügen über eine sehr geringe Maximallänge für Meldungen, z. B. 200 Zeichen. Wenn eine Meldung über eine E-Mail-Adresse an einen Pager gesendet werden soll, können Sie durch das Anfügen eines Sternchens (*) an die Adresse selbst festlegen, wo die Meldung abgeschnitten wird und müssen dies nicht dem Pager-Unternehmen überlassen.

- Sie können den Meldungstext auch im Dialogfeld **Warnungs-Manager-Nachrichten** bearbeiten, um sicherzustellen, dass wichtige Informationen in abgeschnittenen Meldungen erhalten bleiben. Kürzen Sie dazu entweder Teile der Meldung ab, oder verschieben Sie wichtige Informationen an den Anfang der Meldung. Lange Dateinamen könnten Sie am Ende der Meldung belassen.

Senden von Warnmeldungen an einen Drucker

Der Warnungs-Manager kann Warnmeldungen an einen Drucker senden, um sie dort auszudrucken. So konfigurieren Sie den Warnungs-Manager, um Warnmeldungen an die Warteschlange eines Druckers zu senden:

1. Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.
2. Klicken Sie auf die Registerkarte **Drucker**.

   Die Seite **Drucker** wird angezeigt. Sie enthält eine Liste der Druckerwarteschlangen, die für den Empfang von Warnmeldungen ausgewählt wurden. Wenn noch keine Druckerwarteschlange ausgewählt wurde, enthält die Liste keine Einträge.



Abbildung 6-17. Eigenschaften des Warnungs-Managers – Registerkarte "Drucker"

3 Um die Liste zu aktualisieren, können Sie folgendermaßen vorgehen:

- Um der Liste eine Druckerwarteschlange hinzuzufügen, klicken Sie auf **Hinzufügen**. Das Dialogfeld **Eigenschaften von Drucker** wird aufgerufen. Geben Sie den Namen der Druckerwarteschlange ein, an die Meldungen gesendet werden sollen. Sie können den Namen der Druckerwarteschlange eingeben oder auf **Durchsuchen** klicken, um den Drucker im Netzwerk zu suchen.
- Um eine Druckerwarteschlange aus der Liste zu entfernen, wählen Sie einen der aufgelisteten Drucker, und klicken Sie auf **Entfernen.**
- Um die Konfigurationsoptionen zu ändern, wählen Sie einen der aufgelisteten Drucker aus, und klicken Sie auf **Eigenschaften.** Der Warnungs-Manager ruft das Dialogfeld **Eigenschaften von Drucker** auf. Ändern Sie die Informationen im Textfeld **Drucker** nach Bedarf.



Abbildung 6-18. Druckereigenschaften

4 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Zieldrucker empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

5 Klicken Sie auf **Test**, um eine Testnachricht an den Drucker zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

6 Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Senden von Warnmeldungen per SNMP

Der Warnungs-Manager kann Warnmeldungen über SNMP (Simple Network Management Protocol) an andere Computer senden. Um diese Option zu verwenden, müssen Sie auf Ihrem Computer den SNMP-Dienst von Microsoft installieren. Einzelheiten dazu finden Sie in der Dokumentation für Ihr Betriebssystem. Um die von der Client-Virenschutz-Software gesendeten Warnmeldungen anzuzeigen, müssen Sie auch über ein SNMP-Verwaltungssystem verfügen, das mit einem SNMP-Anzeigeprogramm konfiguriert ist. Hinweise zur Einrichtung und Konfiguration des SNMP-Verwaltungssystems finden Sie in der Dokumentation für das entsprechende SNMP-Verwaltungsprodukt.



Abbildung 6-19. SNMP-Warnungen aktivieren

So konfigurieren Sie den Scanner, um Warnmeldungen per SNMP zu senden:

1. Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.
2. Klicken Sie auf die Registerkarte **SNMP**.
3. Wählen Sie **SNMP-Traps aktivieren**.
4. Wenn der Warnungs-Manager auf einem Computer mit dem Betriebssystem Windows NT 4 installiert ist, können Sie auf **SNMP konfigurieren** klicken, um das Windows-Dialogfeld **Netzwerk** anzuzeigen und den SNMP-Dienst von Windows zu konfigurieren. Einzelheiten dazu finden Sie in der Dokumentation für das Betriebssystem.
5. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.
6. Klicken Sie auf **Test**, um per SNMP eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.
7. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Starten eines Programms als Warnung

Immer wenn der Warnungs-Manager eine Warnung über einen gefundenen Virus erhält, kann er automatisch ein beliebiges Programm auf Ihrem Computer oder auf einem beliebigen Computer im Netzwerk starten. Standardmäßig führt der Warnungs-Manager die Datei `VIRNOTFY.EXE` aus, die sich im Installationsordner des Warnungs-Managers befindet. `VIRNOTFY.EXE` zeigt die Namen infizierter Dateien auf dem Computer, auf dem Alert-Manager installiert ist, in einem Dialogfeld mit Bildlaufleiste an.

> **HINWEIS**
> Der Warnungs-Manager startet nur dann ein Programm, wenn er auf Viren bezogene Warnungen erhält. Die Warnmeldung muss die Systemvariablen `%VIRUSNAME%` und `%FILENAME%` enthalten. Siehe *Verwenden von Systemvariablen des Warnungs-Managers* auf Seite 196. Der Warnungs-Manager startet (unabhängig von der für die Programm-Methode eingestellten Prioritätsstufe) nur dann ein Programm, wenn diese Felder in der Warnung enthalten sind. Weitere Informationen zu Prioritätsstufen finden Sie unter *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

So konfigurieren Sie den Warnungs-Manager, damit bei Entdeckung eines Virus ein Programm ausgeführt wird:

1. Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.
2. Klicken Sie auf die Registerkarte **Programm**, um die Seite **Programm** zu öffnen.



Abbildung 6-20. Eigenschaften des Warnungs-Managers – Registerkarte "Programm"

3 Wählen Sie **Programm ausführen**.

4 Geben Sie den Pfad und den Dateinamen des Programms ein, das bei Entdeckung eines Virus durch die Virenschutz-Software ausgeführt werden soll, oder klicken Sie auf **Durchsuchen**, um die Programmdatei im Netzwerk zu suchen.

5 Wählen Sie eine der folgenden Optionen:

- Um das Programm nur dann zu starten, wenn die Virenschutz-Software einen Virus zum ersten Mal findet, klicken Sie auf **Beim ersten Mal**.
- Wenn das Programm jedes Mal gestartet werden soll, wenn der Scanner einen Virus entdeckt, klicken Sie auf **Jedes Mal**.

HINWEIS
Bei Auswahl von **Beim ersten Mal** wird das zugewiesene Programm gestartet, sobald der Scanner einen Virus zum ersten Mal erkennt, z. B. VirusOne. Wenn mehrere Vorkommen von VirusOne im selben Ordner vorhanden sind, wird das Programm nicht nochmals gestartet. Wenn nach VirusOne jedoch erst ein anderer Virus (VirusTwo) und anschließend wieder VirusOne entdeckt wird, wird das Programm für jede Virenerkennung erneut gestartet. Das bedeutet, dass das Programm in diesem Beispiel drei Mal nacheinander gestartet wird. Das Starten mehrerer Instanzen desselben Programms führt ggf. dazu, dass nicht mehr genügend Speicherkapazität zur Verfügung steht.

6 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

Denken Sie daran, dass die Programm-Methode nur dann ein Programm ausführt, wenn die Warnung auf Viren bezogen ist. Die Warnung muss also die Systemvariablen `%VIRUSNAME%` und `%FILENAME%` enthalten. Alle anderen Warnungen werden (unabhängig von der Prioritätsstufe) ignoriert.

7 Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

Protokollieren von Warnbenachrichtigungen im Ereignisprotokoll des Computers

Mit dem Warnungs-Manager können Warnmeldungen im lokalen Ereignisprotokoll Ihres Computers oder im Ereignisprotokoll eines anderen Netzwerkcomputers protokolliert werden.

So konfigurieren Sie die Protokollierungsoptionen:

1 Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.

2 Klicken Sie auf die Registerkarte **Protokollierung**.

Die Seite **Protokollierung** wird angezeigt. Sie enthält eine Liste der Computer, die für den Empfang zu protokollierender Meldungen ausgewählt wurden. Wenn noch kein Empfängercomputer ausgewählt wurde, enthält die Liste keine Einträge.



Abbildung 6-21. Eigenschaften des Warnungs-Managers – Registerkarte "Protokollierung"

3 Um die Liste zu aktualisieren, können Sie folgendermaßen vorgehen:

- Wenn Sie einen Computer hinzufügen möchten, klicken Sie auf **Hinzufügen**, um das Dialogfeld **Protokollierungseigenschaften** aufzurufen, und geben Sie in das Textfeld den Namen des Computers ein, der die weitergeleiteten Meldungen empfangen soll. Der Computername kann entsprechend UNC (Universal Naming Convention) eingegeben werden, oder Sie klicken auf **Durchsuchen**, um den Computer im Netzwerk zu suchen.
- Um einen Computer aus der Liste zu entfernen, wählen Sie einen der aufgelisteten Rechner aus, und klicken Sie auf die Schaltfläche **Entfernen**.

- Um die Konfigurationsoptionen zu ändern, wählen Sie einen der aufgelisteten Empfängercomputer aus, und klicken Sie auf **Eigenschaften.** Der Warnungs-Manager ruft das Dialogfeld **Protokollierungseigenschaften** auf. Geben Sie den Namen des Computers ein, an den die zu protokollierenden Meldungen durch den Warnungs-Manager weitergeleitet werden sollen. Klicken Sie auf **Durchsuchen**, um den Empfängercomputer zu suchen.



Abbildung 6-22. Protokollierungseigenschaften

4. Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.
5. Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.
6. Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Senden einer Netzwerkmeldung an einen Terminalserver

Der Warnungs-Manager kann Warnmeldungen an einen Terminalserver senden. Auf dem Bildschirm des Benutzers, in dessen Sitzung die Warnung erzeugt wurde, werden Popup-Netzwerkmeldungen angezeigt.

Im Dialogfeld **Eigenschaften des Warnungs-Managers** wird die Registerkarte **Terminalserver** nur dann angezeigt, wenn es sich bei dem Computer, auf dem der Warnungs-Manager installiert ist, um einen Terminalserver handelt.

So konfigurieren Sie den Warnungs-Manager für das Senden von Meldungen an einen Terminalserver:

1 Rufen Sie das Dialogfeld **Eigenschaften des Warnungs-Managers** auf.

2 Klicken Sie auf die Registerkarte **Terminalserver**.

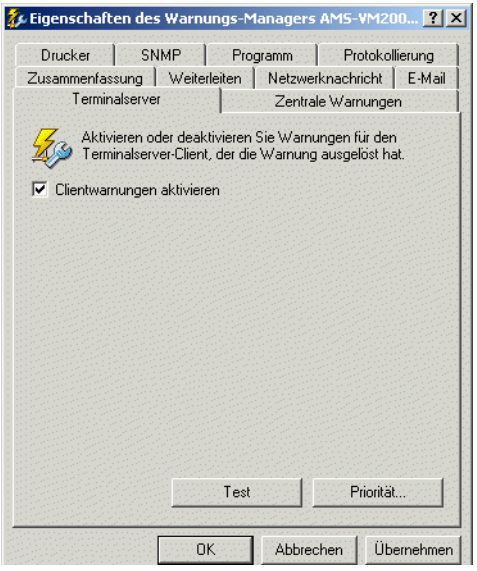


Abbildung 6-23. Eigenschaften des Warnungs-Managers – Registerkarte "Terminalserver"

3 Aktivieren Sie das Kontrollkästchen **Clientwarnungen aktivieren**, um das Senden von Warnmeldungen an den Terminalserver zu aktivieren.

4 Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Das Dialogfeld **Client-Auswahl für Testnachricht** wird angezeigt. Es enthält eine Liste der aktuellen Terminalserver-Benutzersitzungen für diesen Computer.

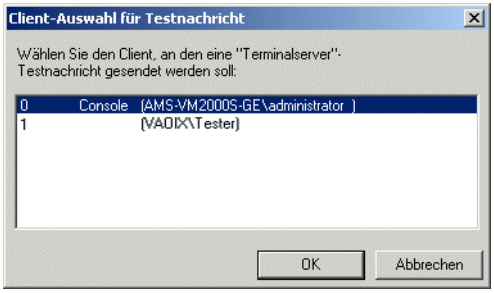


Abbildung 6-24. Senden einer Testnachricht an einen Terminalserverbenutzer

5 Wählen Sie einen Benutzer aus der Liste aus, und klicken Sie auf **OK**, um diesem Benutzer eine Testnachricht zu senden und zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

6 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen die Terminalserverbenutzer empfangen sollen. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

7 Klicken Sie auf **OK**, um die Terminalservereinstellungen zu speichern und zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Verwenden von zentralen Warnungen

Zentrale Warnungen stellen eine Alternative zur regulären Verwendung des Warnungs-Managers beim Versenden von Meldungen dar. Mit der Funktion "Zentrale Warnungen" werden durch Client-Virenschutz-Software (z. B. VirusScan Enterprise) erzeugte Warnmeldungen in einem freigegebenen Ordner auf einem Server gespeichert. Anschließend wird der Warnungs-Manager für das Lesen von Warnbenachrichtigungen aus diesem Ordner konfiguriert. Wenn sich der Inhalt des freigegebenen Ordners ändert, werden vom Warnungs-Manager neue Warnbenachrichtigungen gesendet. Dabei werden die Warnmethoden verwendet, für die der Warnungs-Manager bereits konfiguriert ist. E-Mail-Nachrichten könnten z. B. an einen Pager gesendet werden.

WARNUNG
Auf Grund der Sicherheitsprobleme, die bei freigegebenen Ordnern entstehen können, empfiehlt McAfee Security, die Funktion "Zentrale Warnungen" möglichst *nicht* einzusetzen. Konfigurieren Sie Ihre Client-Virenschutz-Software stattdessen so, dass die regulären Warnmethoden des Warnungs-Managers verwendet werden.

So verwenden Sie die Funktion "Zentrale Warnungen":

1 Um Warnmeldungen an den entsprechenden Warnungsordner zu senden, konfigurieren Sie die Virenschutz-Software auf den Client-Computern. Informationen zur Vorgehensweise finden Sie in der Dokumentation für die Virenschutz-Software.

> **HINWEIS**
> Damit auch andere Arbeitsstationen in Ihrem Netzwerk Meldungen an diesen Ordner senden können, müssen alle Benutzer und Computer über Zugriffsrechte zum *Scannen*, *Schreiben*, *Erstellen* und *Ändern* der Dateien in diesem Ordner verfügen. Einzelheiten dazu finden Sie in der Dokumentation für das Betriebssystem.

2 Vergewissern Sie sich, dass alle Benutzer und Computer Lese- und Schreibzugriff auf den freigegebenen Ordner für Warnungen haben. Wenn sich der Ordner auf einem Computer unter Windows NT befindet, müssen Sie eine Nullsitzungsfreigabe konfigurieren. Einzelheiten dazu finden Sie in der Dokumentation für das Betriebssystem.

3 Konfigurieren Sie den Warnungs-Manager so, dass der Ordner für zentrale Warnungen auf Aktivitäten überwacht wird. Gehen Sie dazu folgendermaßen vor:

   a Klicken Sie im Dialogfeld **Eigenschaften des Warnungs-Managers** auf die Registerkarte **Zentrale Warnung**.



Abbildung 6-25. Eigenschaften für zentrale Warnungen

b Wählen Sie **Zentrale Warnungen aktivieren**.

c Geben Sie den Speicherort des Ordners für Warnungen ein, oder klicken Sie auf **Durchsuchen**, um den Ordner auf dem Server oder im Netzwerk zu suchen. Dabei muss es sich um denselben Ordner handeln, den die Virenschutz-Software auf den Client-Computern für zentrale Warnungen verwendet (siehe Schritt 1). Der Standardspeicherort des Ordners für Warnungen lautet:

C:\Programme\Network Associates\Alert Manager\Queue\.

4 Klicken Sie auf **Prioritätsstufe**, um anzugeben, welche Arten von Warnmeldungen der Empfängercomputer empfangen soll. Siehe *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

5 Klicken Sie auf **Test**, um eine Testnachricht an den Empfängercomputer zu senden. Siehe *Senden einer Testnachricht* auf Seite 168.

6 Klicken Sie auf **OK**, um die Einstellungen für zentrale Warnungen zu speichern und zum Dialogfeld **Eigenschaften des Warnungs-Managers** zurückzukehren.

Anpassen von Warnmeldungen

Im Lieferumfang des Warnungs-Managers ist eine Vielzahl von Warnmeldungen enthalten, die das Spektrum der Situationen bei der Erkennung von Viren auf einem Netzwerkcomputer nahezu vollständig abdecken. Die Warnmeldungen enthalten eine vordefinierte Prioritätsstufe und Systemvariablen, die die infizierte Datei und das infizierte System, den infizierenden Virus und andere Informationen angeben, mit deren Hilfe Sie sich einen ebenso schnellen wie umfassenden Überblick über die Situation verschaffen können.

Um den Funktionsumfang Ihrer spezifischen Situation anzupassen, aktivieren oder deaktivieren Sie bestimmte Warnmeldungen, oder ändern Sie den Inhalt und die Prioritätsstufe einzelner Meldungen. Da die Warnmeldung durch den Warnungs-Manager trotzdem noch als Antwort auf bestimmte auslösende Ereignisse aktiviert wird, sollten Sie sich bei Änderungen bemühen, den Inhalt der Warnmeldung im Wesentlichen beizubehalten.

Zum Anpassen der Warnmeldungen verwenden Sie das Dialogfeld **Warnungs-Manager-Nachrichten**. Informationen zum Zugriff auf das Dialogfeld **Warnungs-Manager-Nachrichten** finden Sie unter *Konfigurieren des Warnungs-Managers* auf Seite 162.


Warnungs-Manager-Nachrichten
Konfigurieren Sie Prioritäten für alle Systemnachrichten, indem Sie die entsprechenden Nachrichten nach Bedarf aktivieren bzw. deaktivieren.
Aktivitätsprotokoll-Fehler. (1040)
Angegebene Medien wurden nicht gefunden. (1044)
Arbeitsspeicher infiziert. (1036)
Aus Scan-Vorgängen auszuschließende Datei. (1029)
Beendigungsanforderung erfolgreich verarbeitet. (151
Beim Scannen wurden infizierte Dateien gefunden un
Beim Scannen wurden infizierte Dateien gefunden. (1
Beim Verschlüsseln der Daten trat ein Fehler auf. (501
Boot-Sektor-Virus wurde gesäubert. (1060)
Das angegebene Scan-Element ist ungültig. (1045)
Das Element kann nicht von Scan-Vorgängen ausges
Das infizierte E-Mail-Element wurde gelöscht. (1504)
Das Upgrade ist fehlgeschlagen (siehe Ereignisprotok
OK
Abbrechen
Bearbeiten...

Abbildung 6-26. Warnungs-Manager-Nachrichten

Hier können die folgenden Aktionen ausgeführt werden:

- Aktivieren und Deaktivieren von Warnmeldungen.
- Bearbeiten von Warnmeldungen.

Aktivieren und Deaktivieren von Warnmeldungen

Mit dem VirusScan Enterprise werden Warnungen ausgegeben, wenn die Virenschutz-Software einen Virus entdeckt oder der normale Betrieb in irgendeiner Weise maßgeblich beeinträchtigt wird. Möglicherweise möchten Sie jedoch nicht in jedem dieser Fälle eine Warnmeldung erhalten. Im Dialogfeld **Warnungs-Manager-Nachrichten** können bestimmte Warnmeldungen deaktiviert werden, die Sie nicht empfangen möchten.

Neben jeder Warnung in der Liste des Dialogfelds **Warnungs-Manager-Nachrichten** befindet sich ein Kontrollkästchen. Bei aktiviertem Kontrollkästchen ist auch die Warnung aktiviert. Dementsprechend ist die Warnung bei deaktiviertem Kontrollkästchen deaktiviert. Standardmäßig sind alle verfügbaren Warnmeldungen aktiviert.

So aktivieren oder deaktivieren Sie Warnmeldungen:

1. Aktivieren bzw. deaktivieren Sie das entsprechende Kontrollkästchen der Warnmeldungen, die aktiviert bzw. deaktiviert werden sollen.
2. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld **Warnungs-Manager-Nachrichten** zu schließen.

Bearbeiten von Warnmeldungen

Beim Bearbeiten von Warnmeldungen stehen Ihnen zwei Möglichkeiten zur Verfügung:

- Ändern der Warnpriorität.
- Bearbeiten des Warnmeldungstexts.

Ändern der Warnpriorität

Einige der Warnungen, die der Warnungs-Manager von der Client-Virenschutz-Software erhält, müssen gegenüber anderen vorrangig behandelt werden. Jeder Warnmeldung ist eine standardmäßige Prioritätsstufe zugewiesen. Diese richtet sich nach der Dringlichkeit, die einer derartigen Warnung von Systemadministratoren in der Regel beigemessen wird. Sie können diese Prioritätsstufen Ihren Anforderungen entsprechend neu zuweisen. Verwenden Sie die Prioritätsstufen, um die Meldungen herauszufiltern, die der Warnungs-Manager an die Empfänger senden soll, sodass diese sich zunächst den wichtigsten Meldungen widmen können.

So ändern Sie die einer Warnmeldung zugewiesene Prioritätsstufe:

1. Klicken Sie im Dialogfeld **Warnungs-Manager-Nachrichten** (siehe *Anpassen von Warnmeldungen* auf Seite 192) einmal auf eine der aufgelisteten Nachrichten, um diese auszuwählen.
2. Klicken Sie auf **Bearbeiten**, um das Dialogfeld **Nachricht des Warnungs-Managers bearbeiten** aufzurufen.

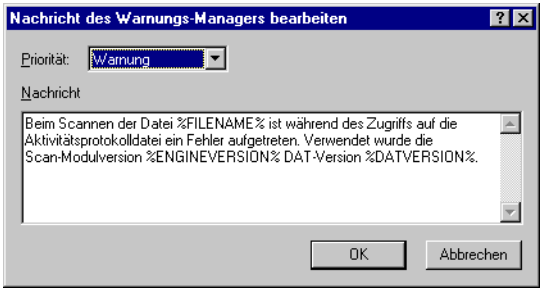

Nachricht des Warnungs-Managers bearbeiten
Priorität:
Warnung
Nachricht
Beim Scannen der Datei %FILENAME% ist während des Zugriffs auf die Aktivitätsprotokolldatei ein Fehler aufgetreten. Verwendet wurde die Scan-Modulversion %ENGINEVERSION% DAT-Version %DATVERSION%.
OK
Abbrechen

Abbildung 6-27. Bearbeiten der Priorität und des Texts einer Warnmeldung

3. Wählen Sie in der Liste **Priorität** eine Prioritätsstufe aus. Den Warnmeldungen können die Prioritätsstufen **Kritisch, Hoch, Gering, Warnung** oder **Information** zugewiesen werden.

   Durch das Symbol neben der im Dialogfeld **Warnungs-Manager-Nachrichten** aufgelisteten Meldung wird die Prioritätsstufe angezeigt, die der Meldung aktuell zugewiesen ist. Jedes Symbol entspricht einer Option in der Dropdown-Liste **Priorität**. Folgende Prioritätsstufen sind verfügbar:

Kritisch. Gibt an, dass die Virenschutz-Software Viren in Dateien erkannt hat, die nicht gesäubert, in den Quarantäneordner verschoben oder gelöscht werden konnten.

Hoch. Gibt an, dass die Erkennung und Säuberung der Viren erfolgreich war oder die Ausführung der Virenschutz-Software auf Grund schwer wiegender Fehler und Probleme möglicherweise abgebrochen wird. Beispiele dafür sind "Die infizierte Datei wurde gelöscht", "Für das angegebene Produkt sind keine Lizenzen installiert" oder "Nicht genügend Speicher!"

Gering. Kennzeichnet Virenerkennungs- oder Statusmeldungen mit niedriger Priorität.

Warnung. Kennzeichnet Statusmeldungen, die wichtiger sind als Informationsmeldungen. Diese Meldungen beziehen sich oft auf unkritische Probleme, die während des Viren-Scans aufgetreten sind.

Information. Kennzeichnet standardmäßige Status- und Informationsmeldungen, z. B. "Scannen bei Zugriff gestartet" oder "Scan-Vorgang abgeschlossen. Keine Viren gefunden".

Wenn Sie einer Meldung eine andere Priorität zuweisen, ändert sich das neben der Meldung angezeigte Symbol, und der neue Prioritätsstatus wird angezeigt.

4 Klicken Sie auf **OK**.

Filtern von Meldungen nach Prioritätsstufe

Um die Meldungen zu filtern, konfigurieren Sie die im Warnungs-Manager eingerichteten Warnmethoden so, dass nur Meldungen mit einer bestimmten Priorität angenommen werden. Beispiel: Sie möchten, dass der Warnungs-Manager immer eine Meldung an Ihren Pager sendet, wenn die Virenschutz-Software in Ihrem Netzwerk einen Virus entdeckt. Routinemäßige Betriebsmeldungen sollen jedoch nicht an Sie gesendet werden. Weisen Sie dazu allen Virus-Warnmeldungen die Priorität *Kritisch* oder *Hoch* und den routinemäßigen Informationsmeldungen die Priorität *Gering*, *Warnung* oder *Information* zu. Anschließend konfigurieren Sie den Warnungs-Manager so, dass an die E-Mail-Adresse für Ihren Pager nur Meldungen mit hoher Priorität gesendet werden.

Informationen zur Anwendung der Prioritätsstufenfilter auf bestimmte Empfänger finden Sie unter *Einrichten der Warnungsprioritätsstufe für Empfänger* auf Seite 169.

Bearbeiten des Warnmeldungstexts

Um Ihnen zu helfen, auf eine Situation zu reagieren, die Ihre Aufmerksamkeit erfordert, enthält der Warnungs-Manager Informationen, die zur Erkennung des Ursprungs eines Problems erforderlich sind, sowie einige Informationen zum Umfeld, in dem das Problem festgestellt wurde. Der Meldungstext kann nach Belieben bearbeitet werden. Sie können der Warnmeldung beispielsweise Kommentare, die das Problem eingehender erörtern, oder Kontaktinformationen zum technischen Support hinzufügen.

> **HINWEIS**
> Obwohl der Warnmeldungstext frei nach Ihren Vorstellungen bearbeitet werden kann, sollte der Inhalt im Wesentlichen beibehalten werden, da der Warnungs-Manager die Meldungen nur in bestimmten Situationen sendet. Die Warnmeldung "Task wurde gestartet" wird beispielsweise nur gesendet, wenn auch tatsächlich ein Task gestartet wird.

So bearbeiten Sie den Text der Warnmeldung:

1. Klicken Sie in der Liste im Dialogfeld **Warnungs-Manager-Nachrichten** auf die Warnmeldung, um diese auszuwählen.
2. Klicken Sie auf **Bearbeiten**, um das Dialogfeld **Nachricht des Warnungs-Managers bearbeiten** aufzurufen.
3. Bearbeiten Sie den Meldungstext Ihren Vorstellungen entsprechend. Bei in Prozentzeichen stehendem Text, z. B. `%COMPUTERNAME%`, handelt es sich um Variablen, die vom Warnungs-Manager entsprechend ersetzt werden, wenn die Warnmeldung erzeugt wird. Siehe *Verwenden von Systemvariablen des Warnungs-Managers* auf Seite 196.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **Warnungseigenschaften** zurückzukehren.

Verwenden von Systemvariablen des Warnungs-Managers

Der Warnungs-Manager 4.7 enthält Systemvariablen, die im Text von Warnmeldungen verwendet werden können. Diese Variablen beziehen sich auf Systemfunktionen wie Datum und Uhrzeit, Dateinamen oder Computernamen. Beim Versenden von Warnbenachrichtigungen werden die Variablen vom Warnungs-Manager dynamisch durch den entsprechenden Wert ersetzt.

Beispiel: Die im Dialogfeld **Warnungs-Manager-Nachrichten** aufgelistete Warnung mit hoher Priorität  *Infizierte Datei wurde erfolgreich gesäubert (1025)* ist standardmäßig wie folgt eingestellt:

```
Die Datei %FILENAME% war mit dem Virus %VIRUSNAME% %VIRUSTYPE%
  infiziert. Die Datei wurde mit der Scan-Modulversion %ENGINEVERSION%
  und mit DAT-Version %DATVERSION% erfolgreich gesäubert.
```

Wenn der Warnungs-Manager diese Warnung von einer Virenschutzanwendung erhält, fügt er tatsächliche Werte in die Systemvariablen ein, z. B. `MEINDOKUMENT.DOC` für die Variable `%FILENAME%`.

Zu den am häufigsten verwendeten Systemvariablen gehören:

`%DATVERSION%`	Version der derzeit von der Virenschutz-Software verwendeten DAT-Dateien, die die Warnung erzeugt hat.
`%ENGINEVERSION%`	Version des derzeitigen Virenschutzmoduls, das von der Virenschutz-Software zum Erkennen einer Infizierung oder anderer Probleme verwendet wird.
`%FILENAME%`	Der Name einer Datei. Dabei kann es sich um den Namen einer erkannten infizierten Datei oder um den Namen einer Datei handeln, die vom Scan-Vorgang ausgeschlossen wurde.
`%TASKNAME%`	Name eines aktiven Tasks, wie z. B. eines Zugriffsscans oder eines AutoUpdate-Tasks in VirusScan Enterprise 7.0. Diese Variable wird vom Warnungs-Manager beispielsweise verwendet, um den Namen eines Tasks anzugeben, durch den der Virus erkannt oder durch den ein Fehler während des Scan-Vorgangs gemeldet wurde.
`%VIRUSNAME%`	Der Name eines infizierenden Virus.
`%DATE%`	Das Systemdatum des Computers, auf dem der Warnungs-Manager installiert ist.
`%TIME%`	Die Systemzeit des Computers, auf dem der Warnungs-Manager installiert ist.
`%COMPUTERNAME%`	Der Name eines Computers, der im Netzwerk vorhanden ist. Dabei kann es sich um einen infizierten Computer, um einen Computer, der einen Gerätetreiberfehler meldet, oder um einen beliebigen anderen Computer handeln, mit dem das Programm interagiert.
`%SOFTWARENAME%`	Der Dateiname einer ausführbaren Datei. Dabei kann es sich um eine Anwendung, die einen Virus erkannt oder einen Fehler gemeldet hat, oder eine beliebige Anwendung handeln, die mit dem Programm interagiert.

%SOFTWAREVERSION%	Die Versionsnummer des aktiven Softwarepakets. Dabei kann es sich um eine Anwendung, die einen Virus erkannt oder einen Fehler gemeldet hat, oder eine beliebige Anwendung handeln, die mit dem Programm interagiert.
%USERNAME%	Der Anmeldename des aktuell beim Server angemeldeten Benutzers. Dadurch kann beispielsweise angezeigt werden, ob der Scan-Vorgang abgebrochen wurde.

WARNUNG
Beim Bearbeiten von Meldungstext zum Hinzufügen von Systemvariablen, die möglicherweise nicht von dem Ereignis verwendet werden, das die Warnmeldung erzeugt, sollten Sie mit größter Vorsicht vorgehen. Das Verwenden von Systemvariablen in Warnungen, die dieses Feld für Systemvariablen nicht verwenden, kann zu unerwarteten Ergebnissen führen, wie z. B. einer Beschädigung des Meldungstextes oder sogar einem Systemabsturz.

In der folgenden Liste sind alle Systemvariablen aufgeführt, die in Warnungs-Manager-Meldungen verwendet werden können:

%ACCESSPROCESSNAME%	%NOTEID%	%RESOLUTION%
%CLIENTCOMPUTER%	%NOTESDBNAME%	%SCANRETURNCODE%
%COMPUTERNAME%	%NOTESSERVERNAME%	%SEVERITY%
%DATVERSION%	%LANGUAGECODE%	%SHORTDESCRIPT%
%DOMAIN%	%LOCALDAY%	%SOFTWARENAME%
%ENGINESTATUS%	%LOCALHOUR%	%SOFTWAREVERSION%
%ENGINEVERSION%	%LOCALMIN%	%SOURCEIP%
%EVENTNAME%	%LOCALMONTH%	%SOURCEMAC%
%FILENAME%	%LOCALSEC%	%SOURCESEG%
%GMTDAY%	%LOCALTIME%	%TARGETCOMPUTERNAME%
%GMTHOUR%	%LOCALYEAR%	%TARGETIP%
%GMTMIN%	%LONGDESCRIPT%	%TARGETMAC%
%GMTMONTH%	%MAILCCNAME%	%TASKID%
%GMTSEC%	%MAILFROMNAME%	%TASKNAME%
%GMTTIME%	%NUMCLEANED%	%TRAPID%
%GMTYEAR%	%NUMDELETED%	%TSCLIENTID%
%INFO%	%NUMQUARANTINED%	%URL%
%MAILIDENTIFIERINFO%	%NUMVIRS%	%USERNAME%
%MAILSUBJECTLINE%	%OBRULENAME%	%VIRUSNAME%
%MAILTONAME%	%OS%	%VIRUSTYPE%
	%PROCESSORSERIA%	

Aktualisieren 7

Die Virenerkennung der VirusScan Enterprise-Software basiert auf den Informationen in den Virusdefinitionsdateien (DAT-Dateien). Ohne aktualisierte Dateien werden neue Viren ggf. nicht durch die Software erkannt bzw. nicht wirksam behandelt. Wenn von der Software keine aktuellen DAT-Dateien verwendet werden, ist die Funktionstüchtigkeit des Virenschutzprogramms gefährdet.

Neue Viren entstehen mit einer Geschwindigkeit, die sich auf mehr als 500 pro Monat beläuft. Um diesem Problem zu begegnen, gibt McAfee Security wöchentlich neue DAT-Dateien heraus, bei deren Erstellung die Ergebnisse der laufenden Forschungen zu den Merkmalen neuer oder mutierter Viren einbezogen werden. Das Feature AutoUpdate erleichtert die Nutzung dieses Diensts. Es ermöglicht Ihnen, mithilfe einer sofortigen oder einer geplanten Aktualisierung die neuesten DAT-Dateien, das aktuelle Scan-Modul und die Datei EXTRA.DAT gleichzeitig herunterzuladen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Aktualisierungsstrategien
- Systemvariablen
- AutoUpdate-Tasks
- AutoUpdate-Repository-Liste
- Spiegelungstasks
- Rollback für DAT-Dateien
- Manuelle Aktualisierungen

Aktualisierungsstrategien

Zur Durchführung von Aktualisierungen stehen verschiedenen Methoden zur Verfügung: Sie können mit den Verwaltungstools Aktualisierungs-Tasks, manuelle Aktualisierungen, Anmeldeskriptes oder geplante Aktualisierungen ausführen. In diesem Dokument werden die mit VirusScan Enterprise gelieferten Aktualisierungstools und die manuelle Aktualisierung beschrieben. Andere Implementierungsformen werden in diesem Dokument nicht erläutert.

Zu einer effizienten Aktualisierungsstrategie gehört in der Regel, dass die Aktualisierungen von der Network Associates-Downloadsite wenigstens von einem Client oder Server Ihres Unternehmens abgerufen werden. Von dort können die Dateien repliziert und im Unternehmen verteilt werden, so dass auch alle anderen Computer Zugriff darauf erhalten. Idealerweise sollten Sie den Umfang der in Ihrem Netzwerk übertragenen Daten reduzieren, indem Sie das Kopieren der aktualisierten Dateien an Ihre Verteilungspunkte automatisieren.

Für eine effiziente Aktualisierung müssen vor allem die Anzahl der Clients und die Anzahl der Standorte berücksichtigt werden. Ein weiterer Aspekt, der das Aktualisierungsschema beeinflusst, ist z. B. die Anzahl der Systeme an den entfernten Standorten und deren Art des Internetzugangs. Die grundlegenden Konzepte zur Populierung der Verteilungspunkte und zur Aktualisierungsplanung betreffen jedoch Unternehmen jeder Größe.

Mit einem Aktualisierungs-Task können Sie folgende Aufgaben ausführen:

- Sie können die Aktualisierung der DAT-Dateien im Netzwerk so planen, dass sie zu geeigneten Zeiten und mit minimalen Eingriffen seitens der Administratoren oder Netzwerkbenutzer erfolgen. Die Aktualisierungs-Tasks können beispielsweise gestaffelt werden; oder Sie richten einen Zeitplan ein, nach dem die Aktualisierungen der DAT-Dateien in den verschiedenen Teilen des Netzwerks stufenweise oder turnusmäßig durchgeführt werden.

- Die administrativen Aufgaben der Aktualisierung können auf mehrere Server oder Domänen-Controller, auf verschiedene Regionen von WANs (Weitverkehrsnetzen) oder auf andere Netzwerkeinheiten verteilt werden. Ein vorwiegend netzinterner Datenverkehr für die Aktualisierung verringert zudem die Wahrscheinlichkeit von Sicherheitslücken im Netzwerk.

- Sie können weitgehend verhindern, dass beim Herunterladen neuer DAT- oder Upgrade-Moduldateien Wartezeiten entstehen. Zu den regulären Terminen für die Veröffentlichung von DAT-Dateien oder beim Erscheinen neuer Produktversionen erhöht sich der Verkehr auf McAfee-Computern erfahrungsgemäß besonders stark. Wenn Sie diese Spitzenzeiten umgehen, in denen die verfügbare Bandbreite stark beschränkt ist, können Sie die neue Software mit minimalen Unterbrechungen bereitstellen.

Weitere Informationen über das Aktualisieren und Verwenden von McAfee Installation Designer oder McAfee AutoUpdate Architect für die Konfiguration und Verwaltung von Updates finden Sie im *VirusScan Enterprise Implementierungshandbuch für Aktualisierungen*.

Systemvariablen

Systemvariablen werden für die Pfaddefinition bei der Konfiguration von AutoUpDate-Tasks, Spiegelungstasks und Repositories unterstützt. Zu den am häufigsten verwendeten Systemvariablen gehören:

Variable	Definition
<COMPUTER_NAME>	Der Name des Computers, wie er im Netzwerk angezeigt wird.
<USER_NAME>	Der Anmeldename des aktuell am Computer angemeldeten Benutzers.
<DOMAIN_NAME>	Der Name der Domäne.
<SYSTEM_DRIVE>	Der Name der Systemlaufwerks. Zum Beispiel: `C:`
<SYSTEM_ROOT>	Der Pfad zum Stammverzeichnis. Zum Beispiel: `C:\WinNT`
<SYSTEM_DIR>	Der Pfad zum Systemverzeichnis. Zum Beispiel: `C:\WinNT\System32`
<TEMP_DIR>	Der Pfad zum Temporärverzeichnis. Zum Beispiel: `C:\Dokumente und Einstellungen\Administrator\Lokale Einstellungen\Temp`
<PROGRAM_FILES_DIR>	Der Pfad zum Programmeverzeichnis. Zum Beispiel: `C:\Programme`
<PROGRAM_FILES_COMMON_DIR>	Der Pfad zum Verzeichnis "Gemeinsame Dateien". Zum Beispiel: `C:\Programme\Gemeinsame Dateien`
<SOFTWARE_INSTALLED_DIR>	Der Pfad zum Speicherort, an dem die Software installiert ist.
<PP_VAR_NAME>	McAfee-Produktvariablenname. Zum Beispiel: `%ALLUSERSPROFILE%`

AutoUpdate-Tasks

Der AutoUpdate-Task wird verwendet, um geplante oder sofortige Aktualisierungen auszuführen. Sie können DAT-Dateien, das Scan-Modul und die Datei EXTRA.DAT aktualisieren. Informationen über den Download von HotFix-, Service Pack-, SuperDAT-Paket oder .CAB-Dateien finden Sie im *VirusScan EnterpriseImplementierungshandbuch für Aktualisierungen*.

VirusScan Enterprise enthält standardmäßig einen Aktualisierungs-Task, der jeweils freitags um 17:00 (mit bis zu einer Stunde Abweichung) eine Aktualisierung ausführt. Der standardmäßig ausgeführte Aktualisierungs-Task hat den Namen **AutoUpdate**; er kann umbenannt und neu konfiguriert werden. Sie können Ihren Anforderungen entsprechend auch weitere Aktualisierungs-Tasks erstellen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Übersicht über die AutoUpdate-Tasks
- Erstellen eines AutoUpdate-Tasks
- Konfigurieren eines AutoUpdate-Tasks
- Ausführen von AutoUpdate-Tasks
- Anzeigen des Aktivitätsprotokolls

Übersicht über die AutoUpdate-Tasks

Im folgenden Diagramm sehen Sie eine Übersicht über einen AutoUpdate-Task:

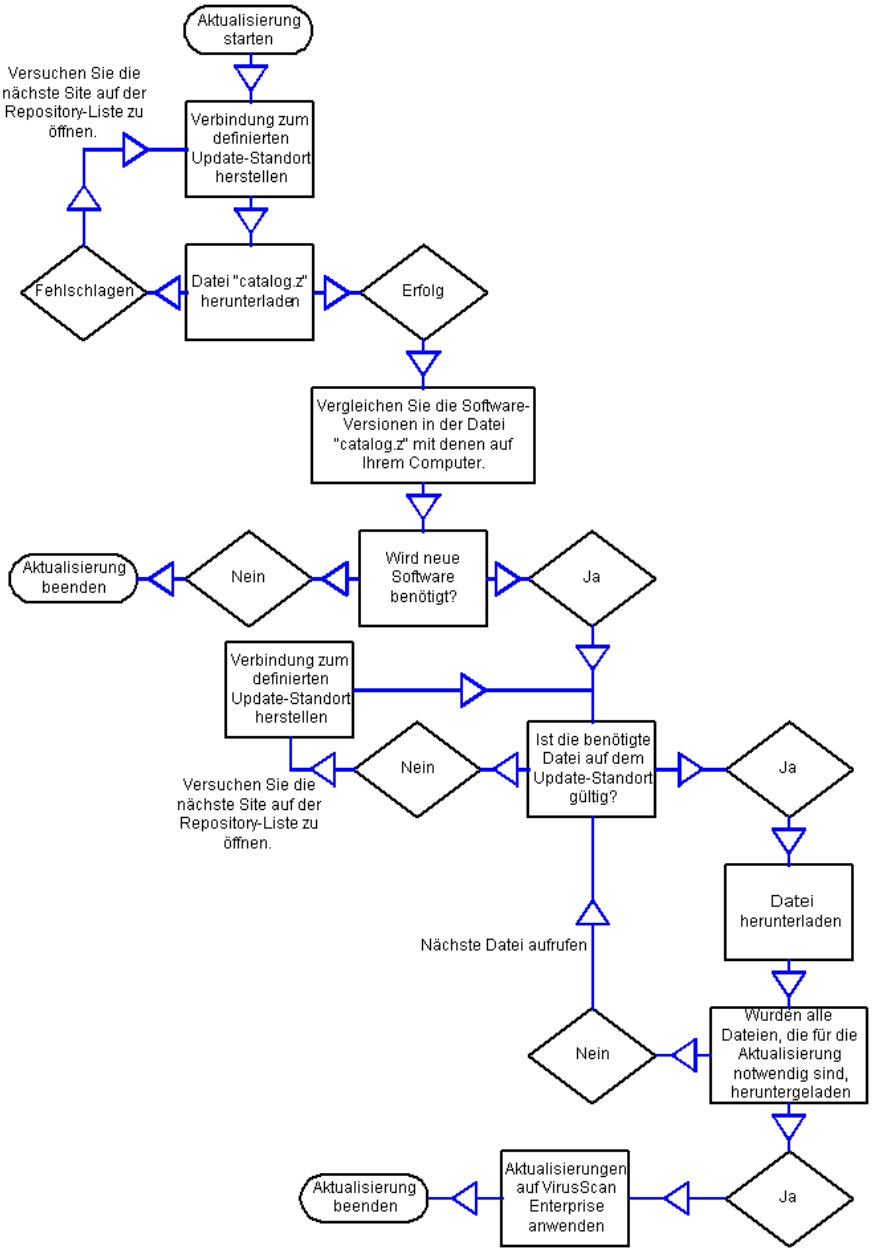

Aktualisierung starten
Versuchen Sie die nächste Site auf der Repository-Liste zu öffnen.
Verbindung zum definierten Update-Standort herstellen
Fehlschlagen
Datei "catalog.z" herunterladen
Erfolg
Vergleichen Sie die Software-Versionen in der Datei "catalog.z" mit denen auf Ihrem Computer.
Aktualisierung beenden
Nein
Wird neue Software benötigt?
Ja
Verbindung zum definierten Update-Standort herstellen
Nein
Versuchen Sie die nächste Site auf der Repository-Liste zu öffnen.
Ist die benötigte Datei auf dem Update-Standort gültig?
Ja
Datei herunterladen
Nächste Datei aufrufen
Nein
Wurden alle Dateien, die für die Aktualisierung notwendig sind, heruntergeladen
Ja
Aktualisierungen auf VirusScan Enterprise anwenden
Aktualisierung beenden

Abbildung 7-1. Übersicht über die AutoUpdate-Tasks

Erstellen eines AutoUpdate-Tasks

So erstellen Sie einen neuen AutoUpdate-Task:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Erstellen Sie einen neuen Aktualisierungs-Task mithilfe einer der folgenden Methoden:
   - Klicken Sie mit der rechten Maustaste in einen leeren Bereich der Konsole, *ohne ein Element in der Taskliste zu markieren*. Wählen Sie dann **Neuer Aktualisierungs-Task**.
   - Wählen Sie aus dem Menü **Task** die Option **Neuer Aktualisierungs-Task**.

     In der Taskliste der **VirusScan-Konsole** wird ein neuer Aktualisierungs-Task markiert angezeigt.
3. Übernehmen Sie den Standard-Task-Namen oder geben Sie einen neuen Namen für diesen Task ein und drücken Sie dann die EINGABETASTE, um das Dialogfeld **Eigenschaften von VirusScan AutoUpdate** zu öffnen. Ausführliche Konfigurationsinformationen finden Sie unter *Konfigurieren eines AutoUpdate-Tasks* auf Seite 204.

HINWEIS
Wenn Sie Aktualisierungs-Tasks über ePolicy Orchestrator 3.0 oder höher erstellen und Tasksichtbarkeit aktivieren, sind diese Aktualisierungs-Tasks in der VirusScan-Konsole sichtbar. Auf diese ePolicy Orchestrator-Tasks besteht nur *Lesezugriff* und sie können nicht von der VirusScan-Konsole aus konfiguriert werden. Weitere Informationen finden Sie im *VirusScan Enterprise Konfigurationshandbuch für die Verwendung mit ePolicy Orchestrator 3.0*.

Konfigurieren eines AutoUpdate-Tasks

Sie können einen AutoUpdate-Task Ihren Anforderungen entsprechend konfigurieren und planen.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Öffnen Sie das Dialogfeld **Eigenschaften von AutoUpdate**. Verwenden Sie dabei eine der folgenden Vorgehensweisen:
   - Markieren Sie den Task in der Taskliste der Konsole und wählen Sie dann aus dem Menü **Task** die Option **Eigenschaften**.
   - Doppelklicken Sie in der Taskliste auf den Task.

- Klicken Sie mit der rechten Maustaste in der Taskliste auf den Task und wählen Sie anschließend **Eigenschaften**.
- Markieren Sie den Task in der Taskliste und klicken Sie auf .

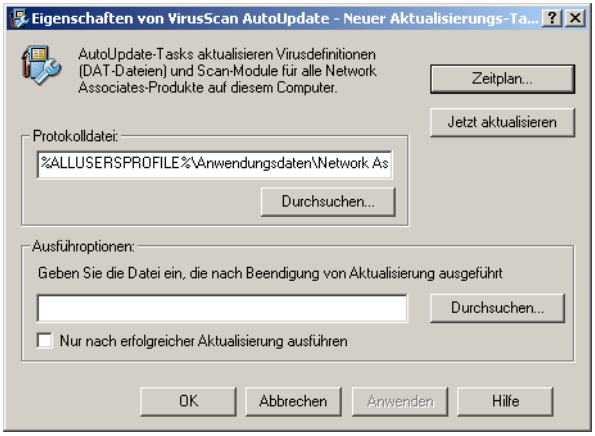


Abbildung 7-2. Eigenschaften von VirusScan AutoUpdate – Neuer Aktualisierungs-Task

HINWEIS
Konfigurieren Sie den Aktualisierungs-Task, bevor Sie auf **Zeitplan** oder **Jetzt aktualisieren** klicken.

3 Sie können den im Textfeld **Protokolldatei** angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einem anderen geeigneten Speicherort zu wechseln. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201.

HINWEIS
Standardmäßig werden Protokollinformationen in die Datei UPDATELOG.TXT in diesem Ordner geschrieben:

```
<Laufwerk>:Winnt\Profiles\All Users\Application
Data\Network Associates\VirusScan
```

4 Unter **Ausführoptionen** können Sie eine ausführbare Datei angeben, die ausgeführt wird, nachdem der **AutoUpdate**-Task abgeschlossen ist. Sie können mit dieser Option z. B. ein Dienstprogramm für Netzwerkmeldungen starten, so dass der Administrator benachrichtigt wird, dass der Aktualisierungsvorgang erfolgreich abgeschlossen wurde.

- **Geben Sie die ausführbare Datei an, die nach Abschluss des Aktualisierungs-Tasks ausgeführt werden soll**. Geben Sie den Pfad zu der auszuführenden Datei ein oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.

- **Nur nach erfolgreicher Aktualisierung ausführen**. Das ausführbare Programm wird nur nach einer erfolgreichen Aktualisierung ausgeführt. Wenn die Aktualisierung jedoch fehlschlägt, wird die angegebene Programmdatei nicht ausgeführt.

  HINWEIS
  Die angegebene Programmdatei muss vom derzeit angemeldeten Benutzer ausgeführt werden können. Wenn der derzeit angemeldete Benutzer über keine Zugriffsrechte auf das Verzeichnis mit den Programmdateien verfügt bzw. wenn zur Zeit keine Benutzer angemeldet sind, wird das Programm nicht ausgeführt.

5. Klicken Sie auf **Zeitplan**, um den Aktualisierungs-Task zu planen. Weitere Informationen finden Sie unter *Planen von Tasks* auf Seite 235.
6. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
7. Klicken Sie auf **Jetzt aktualisieren**, um den Aktualisierungs-Task sofort zu starten.
8. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften von VirusScan AutoUpdate** zu schließen.

   HINWEIS
   Der Aktualisierungs-Task verwendet die Konfigurationseinstellungen in der AutoUpdate-Repository-Liste, um die Aktualisierung auszuführen. Weitere Informationen finden Sie unter *AutoUpdate-Repository-Liste* auf Seite 210.

Ausführen von AutoUpdate-Tasks

Nachdem Sie den Task mit den gewünschten Aktualisierungseigenschaften konfiguriert haben, können Sie den Aktualisierungs-Task ausführen. In diesem Abschnitt werden die folgenden Themen behandelt:

- Ausführen von Aktualisierungs-Tasks
- Aktivitäten während eines Aktualisierungs-Tasks

Ausführen von Aktualisierungs-Tasks

Aktualisierungen können bei Bedarf sofort oder zu einem geplanten Termin ausgeführt werden. Wenn der Aktualisierungs-Task während der Ausführung unterbrochen wird, wird er automatisch wie folgt fortgesetzt:

- **Tasks, die von einer HTTP-, UNC-, oder einer lokalen Site aktualisieren**: Wenn der Aktualisierungs-Task aus bestimmten Gründen unterbrochen wird, wird der Task beim nächsten Start an dieser Stelle wieder aufgenommen.

- **Tasks, die von einer FTP-Site aktualisieren**: Der Task wird nicht wieder aufgenommen, wenn er während des Downloads einer einzelnen Datei unterbrochen wird. Wenn ein Task jedoch mehrere Dateien herunterlädt und unterbrochen wird, wird der Task bei der Datei wieder aufgenommen, die vor der Unterbrechung heruntergeladen wurde.

So führen Sie einen Aktualisierungs-Task aus:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie den Aktualisierungs-Task anhand einer der folgenden Methoden aus:
   - **Aktualisieren nach Zeitplan**: Wenn die Aktualisierung zeitlich geplant wurde, können Sie den Task unbeaufsichtigt ausführen lassen.

     HINWEIS
     Der Computer muss zum Ausführen des Tasks eingeschaltet sein. Wenn der Computer zum Zeitpunkt der geplanten Ausführung des Tasks heruntergefahren ist, wird der Task entweder zum nächsten geplanten Zeitpunkt gestartet, zu dem der Computer eingeschaltet ist, oder wenn der Computer neu gestartet wird. Hierfür muss jedoch auf der Registerkarte **Zeitplan** unter **Zeitplaneinstellungen** die Option **Ausgelassenen Task ausführen** aktiviert sein.

   - **Sofortiges Aktualisieren**: Zum sofortigen Starten von Aktualisierungs-Tasks stehen Ihnen drei Methoden zur Verfügung:
     - Befehl **Jetzt aktualisieren** für die Standard-Aktualisierungs-Task
     - Befehl **Start** für alle Aktualisierungs-Tasks
     - Befehl **Jetzt aktualisieren** für alle Aktualisierungs-Tasks

Befehl "Jetzt aktualisieren" für die Standard-Aktualisierungs-Task

Verwenden Sie die Option **Jetzt aktualisieren**, um den standardmäßig eingerichteten Aktualisierungs-Task sofort zu starten.

HINWEIS
Die Option **Jetzt aktualisieren** führt nur den Standard-Aktualisierungs-Task aus, der beim Installieren des Produkts erstellt wurde. Sie können den Standard-Task umbenennen und neu konfigurieren. Wenn Sie den Task jedoch löschen, wird die Option **Jetzt aktualisieren** deaktiviert.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Um eine sofortige Aktualisierung mit **Jetzt aktualisieren** auszuführen, verwenden Sie eine der folgenden Vorgehensweisen:

- Wählen Sie aus dem Menü **Task** in der **VirusScan-Konsole** die Option **Jetzt aktualisieren**.
- Klicken Sie mit der rechten Maustaste auf  in der Systemablage und wählen Sie anschließend **Jetzt aktualisieren**.

3 Wenn der Task abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee Updater** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

Start-Befehl für alle Aktualisierungs-Tasks

Verwenden Sie in der **VirusScan-Konsole** die Option **Starten**, um einen Aktualisierungs-Task sofort zu beginnen.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Um eine sofortige Aktualisierung aus der **VirusScan-Konsole** zu starten, verwenden Sie eine der folgenden Vorgehensweisen:

- Markieren Sie den Task in der Taskliste der Konsole und wählen Sie dann aus dem Menü **Task** die Option **Starten**.
- Klicken Sie mit der rechten Maustaste in der Taskliste auf den Task und wählen Sie anschließend **Starten**.
- Markieren Sie den Task in der Taskliste und klicken Sie auf  .

3 Wenn der Task abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee Updater** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

Befehl "Jetzt aktualisieren" für alle Aktualisierungs-Tasks

Verwenden Sie im Dialogfeld **Eigenschaften von VirusScan AutoUpdate** die Option **Jetzt aktualisieren**, um alle Aktualisierungs-Tasks sofort zu beginnen.

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Öffnen Sie für den ausgewählten Aktualisierungs-Task das Dialogfeld **Eigenschaften von VirusScan AutoUpdate**. Anleitungen finden Sie unter *Konfigurieren eines AutoUpdate-Tasks* auf Seite 204.

3 Klicken Sie im Dialogfeld **Eigenschaften von VirusScan AutoUpdate** auf **Jetzt aktualisieren**.

4 Wenn der Task abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee Updater** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

Aktivitäten während eines Aktualisierungs-Tasks

Folgende Aktivitäten werden während eines AutoUpdate-Tasks ausgeführt:

- Es wird eine Verbindung zum ersten *aktivierten* Repository (Update-Standort) in der Repository-Liste hergestellt. Wenn dieses Repository nicht verfügbar ist, wird versucht, eine Verbindung zum nächsten Repository herzustellen usw., bis eine Verbindung hergestellt werden kann oder das Ende der Liste erreicht ist.
- Die verschlüsselte Datei CATALOG.Z wird aus dem Repository heruntergeladen. Die Datei CATALOG.Z enthält die wichtigsten Daten für die Durchführung der Aktualisierung. Diese Daten werden verwendet, um zu ermitteln, welche Dateien und/oder Aktualisierungen verfügbar sind.
- Die Software-Versionen in CATALOG.Z werden mit den Versionen auf dem Computer verglichen. Wenn neue Software-Aktualisierungen verfügbar sind, werden sie heruntergeladen.
- Wenn die Aktualisierung in das Repository eingecheckt wurde, wird das Update überprüft, um zu bestätigen, dass es auf VirusScan Enterprise angewendet werden kann und die Version neuer ist als die aktuelle Version. Sobald dies überprüft wurde, lädt VirusScan Enterprise die Aktualisierung herunter, wenn der nächste Aktualisierungs-Task ausgeführt wird.

Eine Datei mit dem Namen EXTRA.DAT kann im Notfall verwendet werden, um neue Bedrohungen zu erkennen, bis der neue Virus zur wöchentlich aktualisierten Virusdefinitionsdatei hinzugefügt wurde. Die Datei EXTRA.DAT wird bei jeder Aktualisierung aus dem Repository heruntergeladen. Dadurch wird gewährleistet, dass bei einer Bearbeitung der Datei EXTRA.DAT und einem erneuten Einchecken dieser Datei als Paket alle VirusScan Enterprise-Clients dasselbe aktualisierte EXTRA.DAT-Paket herunterladen und verwenden. Sie können die Datei EXTRA.DAT beispielsweise als verbesserten Detektor für dasselbe Virus verwenden oder als zusätzlichen Detektor für neue Viren. VirusScan Enterprise unterstützt nur eine (1) Datei EXTRA.DAT.

HINWEIS

Wenn Sie die Arbeit mit der Datei EXTRA.DAT beendet haben, sollten Sie sie aus dem Master-Repository entfernen und einen Replizierungs-Task durchführen, um zu gewährleisten, dass sie aus allen verteilten Repository-Sites entfernt wird. So wird verhindert, dass VirusScan Enterprise-Clients versuchen, die Datei EXTRA.DAT bei einem Akualisierungsvorgang herunterzuladen.

Standardmäßig wird die Entdeckung des neuen Virus in der Datei EXTRA.DAT ignoriert, sobald die neue Virusdefinition in die wöchentlichen DAT-Dateien aufgenommen wurde.

Ein Diagramm zum Aktualisierungsvorgang finden Sie unter *Übersicht über die AutoUpdate-Tasks* auf Seite 203.

Anzeigen des Aktivitätsprotokolls

Das Aktivitätsprotokoll für Aktualisierungs-Tasks zeigt spezifische Details zum Aktualisierungsvorgang an. So werden z. B. die Versionsnummern der aktualisierten DAT-Datei und des Scan-Moduls angezeigt.

So zeigen Sie das Aktivitätsprotokoll an:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Öffnen Sie die Aktivitätsprotokolldatei anhand einer der folgenden Methoden:
   - Markieren Sie den Task und wählen Sie dann aus dem Menü **Task** die Option **Aktivitätsprotokoll**.
   - Klicken Sie mit der rechten Maustaste auf den Task in der Taskliste und wählen Sie die Option **Protokoll anzeigen**.
3. Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

AutoUpdate-Repository-Liste

Die AutoUpdate-Repository-Liste (SITELIST.XML) gibt die zur Ausführung eines Aktualisierungs-Tasks erforderlichen Repositories und Konfigurationsdaten an.

Zum Beispiel:

- Repository-Informationen und -Standort
- Bevorzugte Repository-Reihenfolge
- Proxy-Einstellungen (sofern erforderlich)
- Für den Zugriff auf die einzelnen Repositories erforderliche Anmeldedaten

  HINWEIS
  Diese Anmeldedaten sind verschlüsselt.

Die AutoUpdate-Repository-Liste (SITELIST.XML) befindet sich je nach Betriebssystem an unterschiedlichen Speicherorten.

Z. B. unter Windows NT:

```
C:\Programme\Network Associates\Common Framework\Data
```

Z. B. unter Windows 2000:

```
C:\Dokumente und Einstellungen\Alle
Benutzer\Anwendungsdaten\Network Associates\Common Framework
```

In diesem Abschnitt werden die folgenden Themen behandelt:

- AutoUpdate-Repositories
- Konfigurieren der AutoUpdate-Repository-Liste

AutoUpdate-Repositories

Ein Repository ist ein Speicherort, von dem Sie Aktualisierungen erhalten.

Die Software VirusScan Enterprise ist bei Auslieferung mit zwei Repositories vorkonfiguriert:

ftp://ftp.nai.com/CommonUpdater

http://update.nai.com/Products/CommonUpdater

Das FTP-Repository ist die Standard-Site. Wenn Sie planen, das FTP-Repository zu verwenden, um Aktualisierungen auszuführen, ist dies nach Abschluss des VirusScanEnterprise 7.1.0-Installationsvorgangs automatisch konfiguriert.

Sie können jede dieser Sites verwenden, um die neuesten Aktualisierungen herunterzuladen, wenn Sie ausschließlich VirusScanEnterprise 7.1.0 verwenden oder wenn Sie VirusScanEnterprise 7.1.0 in einer gemischten Umgebung mit VirusScan 4.5.1 oder NetShield 4.5 verwenden.

Sie können die Repositories in der Liste neu organisieren oder neue Repositories Ihren Anforderungen entsprechend erstellen. Die Anzahl der Repositories, die Sie benötigen, hängt von Ihren Aktualisierungsanforderungen ab. Weitere Informationen finden Sie unter *Bearbeiten der AutoUpdate-Repository-Liste* auf Seite 213.

Konfigurieren der AutoUpdate-Repository-Liste

Sie können die AutoUpdate-Repository-Liste (SITELIST.XML) vor, während oder nach der Installation konfigurieren.

In diesem Handbuch werden die Optionen nach der Installation besprochen. Weitere Informationen zu den Installationsoptionen finden Sie im *VirusScan Enterprise Implementierungshandbuch für Aktualisierungen*.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Importieren der AutoUpdate-Repository-Liste
- Bearbeiten der AutoUpdate-Repository-Liste

Importieren der AutoUpdate-Repository-Liste

So importieren Sie eine AutoUpdate-Repository-Liste aus einem anderen Verzeichnis:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Wählen Sie die Option **Extras** | **AutoUpdate-Repository-Liste importieren**.



Abbildung 7-3. AutoUpdate-Repository-Liste importieren

3 Geben Sie im Feld **Suchen in** das Verzeichnis für die .XML-Datei ein oder klicken Sie auf , um zu dem Verzeichnis zu navigieren, und wählen Sie dann die Datei aus.

4 Klicken Sie auf **Öffnen**, um die AutoUpdate-Repository-Liste zu importieren.

HINWEIS
Um eine angepasste AutoUpdate-Repository-Liste zu importieren, um Quell-Repositories anzugeben, aus denen die Software bezogen wird, oder um mehrere Aktualisierungsverzeichnisse zu verwenden, die von einem Master-Repository repliziert werden können, müssen Sie das Dienstprogramm McAfee AutoUpdate Architect™ in Verbindung mit VirusScan Enterprise verwenden. Weitere Informationen finden Sie im *Produkthandbuch* zu McAfee AutoUpdate Architect.

Bearbeiten der AutoUpdate-Repository-Liste

Im Dialogfeld **AutoUpdate Repository-Liste bearbeiten** können Sie der Liste neue AutoUpdate-Repositories hinzufügen, diese konfigurieren, vorhandene Repositories bearbeiten und entfernen und sie in der Liste anordnen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Hinzufügen und Bearbeiten von Repositories
- Entfernen und Neuorganisieren von Repositories
- Festlegen von Proxy-Einstellungen

Hinzufügen und Bearbeiten von Repositories

In Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** können Sie der Liste AutoUpdate-Repositories hinzufügen oder sie bearbeiten.

> **HINWEIS**
> Sie können Repositories auch mithilfe von McAfee AutoUpdate Architect erstellen und in VirusScan Enterprise exportieren. Weitere Informationen zum Erstellen von AutoUpdate-Repositories mit McAfee AutoUpdate Architect finden Sie im *Produkthandbuch* zu diesem Programm.

AutoUpdate-Repositories können den Status *Aktiviert* oder *Deaktiviert* aufweisen.

- **Aktiviert**: Ein definiertes Repository, das beim AutoUpdate-Vorgang verwendet werden kann.
- **Deaktiviert**: Ein definiertes Repository, auf das beim AutoUpdate-Vorgang nicht zugegriffen werden soll.

So fügen Sie ein Repository in die AutoUpdate-Repository-Liste ein oder bearbeiten es:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie die Option **Extras** | **AutoUpdate-Repository-Liste bearbeiten**.
3. Wählen Sie die Registerkarte **Repositories**. *Das* FTP-*Repository ist die Standard-Download-Site*.

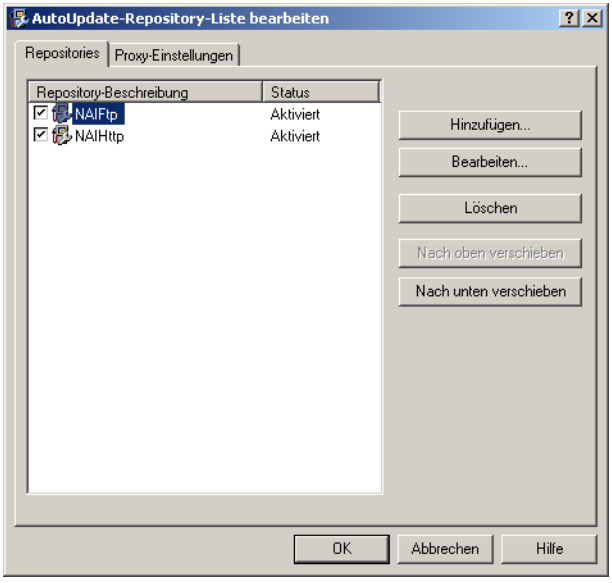


Abbildung 7-4. AutoUpdate-Repository-Liste bearbeiten – Registerkarte "Repositories"

4 Wählen Sie eine der folgenden Aktionen aus:

- Klicken Sie zum Hinzufügen eines Repositories auf **Hinzufügen**. Dadurch wird das Dialogfeld **Repository-Einstellungen** angezeigt.
- Um ein Repository zu bearbeiten, markieren Sie es in der Liste **Repository-Beschreibung** und klicken dann auf **Bearbeiten**, um das Dialogfeld **Repository-Einstellungen** aufzurufen.

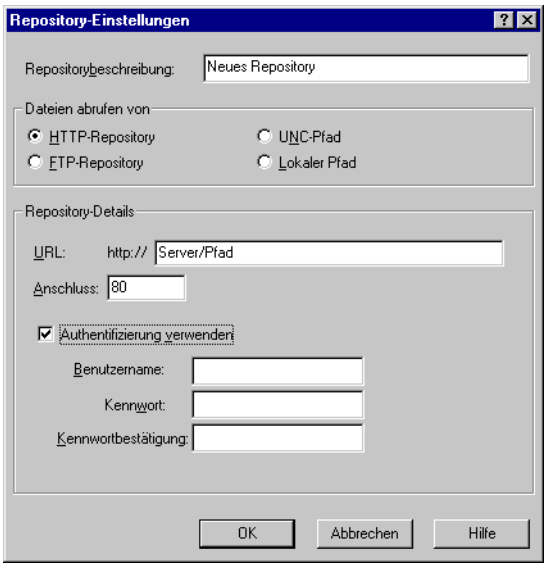


Abbildung 7-5. Repository-Einstellungen

5 Geben Sie im Textfeld **Repository-Beschreibung** den Namen oder eine Beschreibung für dieses Repository ein.

6 Wählen Sie unter **Dateien abrufen von** den Repository-Typ bzw. den Repository-Pfad über eine dieser Optionen aus:

- **HTTP-Repository**: *Diese Option ist standardmäßig ausgewählt.* Verwenden Sie die von Ihnen angegebene HTTP-Repository-Adresse als Repository zum Abrufen der Aktualisierungsdateien.

  HINWEIS
  Eine HTTP-Site, wie beispielsweise FTP, bietet Aktualisierungen unabhängig von der Netzwerksicherheit, unterstützt jedoch eine größere Anzahl von gleichzeitigen Verbindungen als FTP.

- **FTP-Repository**: Verwenden Sie die von Ihnen angegebene FTP-Repository-Adresse als Repository zum Abrufen der Aktualisierungsdateien.

  HINWEIS
  Eine FTP-Site bietet die Flexibilität der Aktualisierung ohne Berücksichtigung der Netzwerk-Sicherheitsrechte. FTP ist weniger anfällig für unerwünschte Code-Angriffe als HTTP, so dass es eine höhere Toleranz bieten kann.

- **UNC-Pfad**: Verwenden Sie den von Ihnen angegebenen UNC-Pfad als das Repository, von dem Sie die Aktualisierungsdateien abrufen.

HINWEIS
Eine UNC-Site lässt sich am schnellsten und einfachsten einrichten. Bei domänenübergreifenden UNC-Aktualisierungen sind Sicherheitsberechtigungen für jede Domäne erforderlich, wodurch die Aktualisierungskonfiguration komplexer wird.

- **Lokaler Pfad**: Verwenden Sie die von Ihnen angegebene lokale Site als das Repository, von dem Sie die Aktualisierungsdateien abrufen.

7 Die Informationen, die Sie unter **Repository-Details** eingeben, hängen vom Repository-Typ bzw. -Pfad ab, den sie unter **Dateien abrufen von** ausgewählt haben. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201. Wählen Sie eine der folgenden Optionen aus:

- Detaillierte Anleitungen für die Optionen **HTTP-Repository** oder **FTP-Repository** finden Sie unter *HTTP- oder FTP-Repository-Details* auf Seite 216.
- Detaillierte Anleitungen für die Optionen **UNC-Pfad** oder **Lokaler Pfad** finden Sie unter *UNC-Pfad oder Lokaler Pfad – Repository-Details* auf Seite 218.

HTTP- oder FTP-Repository-Details

Gehen Sie folgendermaßen vor, wenn Sie ein HTTP- oder FTP-Repository ausgewählt haben:

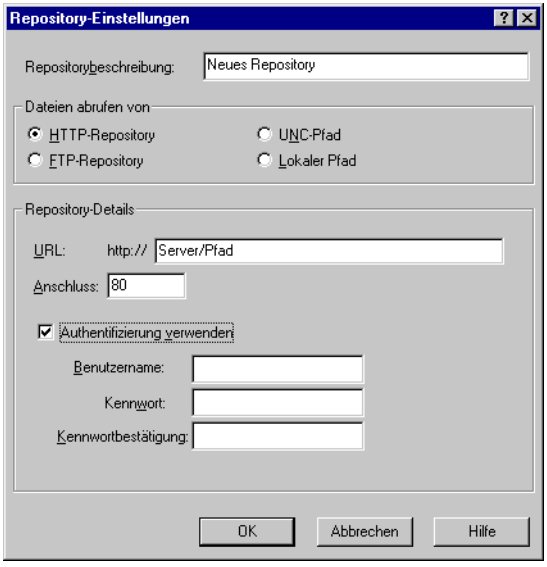


Abbildung 7-6. Repository-Details – HTTP- oder FTP-Site

1 Geben Sie unter **Repository-Details** den Pfad zu dem gewählten Repository, die Portnummer und die Anmeldedaten zum Zugriff auf dieses Repository an.

- **URL**: Geben Sie den Pfad zu der HTTP- oder FTP-Repository-Adresse ein:
  - **HTTP**: Geben Sie den Speicherort für den HTTP-Server und den Ordner an, in dem die Aktualisierungsdateien liegen. Das HTTP-Standard-Repository von McAfee für DAT-Dateien finden Sie unter:

    http://update.nai.com/Products/CommonUpdater
  - **FTP**: Geben Sie den Speicherort für den FTP-Server und den Ordner an, in dem die Aktualisierungsdateien liegen. Das FTP-Standard-Repository von McAfee für DAT-Dateien finden Sie unter:

    ftp://ftp.nai.com/CommonUpdater
- **Port**: Geben Sie die Portnummer für den gewählten HTTP- oder FTP-Server ein.
- **Authentifizierung verwenden** oder **Anonyme Anmeldung verwenden**: *Der Optionsname ist davon abhängig, ob Sie den HTTP-Pfad oder den FTP-Pfad ausgewählt haben.* Geben Sie die Anmeldedaten zum Zugriff auf das Repository an. Geben Sie einen **Benutzernamen** und ein **Kennwort** ein und wiederholen Sie die Eingabe des Kennworts unter **Kennwort bestätigen**.

  HINWEIS
  Anmeldeinformationen zum Herunterladen sind bei FTP- und UNC-Repositories erforderlich, bei HTTP-Repositories optional. AutoUpdate verwendet die angegebenen Anmeldeinformationen für den Zugriff auf das Repository, so dass die benötigten Aktualisierungsdateien heruntergeladen werden können. Beim Konfigurieren der Anmeldeinformationen für das Konto im Repository, müssen Sie darauf achten, dass das Konto *Lese*berechtigungen für die Ordner mit den Aktualisierungsdateien besitzt.

  FTP-Aktualisierungen unterstützen anonyme Repository-Verbindungen.

2 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum Dialogfeld **AutoUpdate-Repository-Liste** zurückzukehren.

UNC-Pfad oder Lokaler Pfad – Repository-Details

Bei Auswahl von "UNC-Pfad" bzw. "Lokaler Pfad":

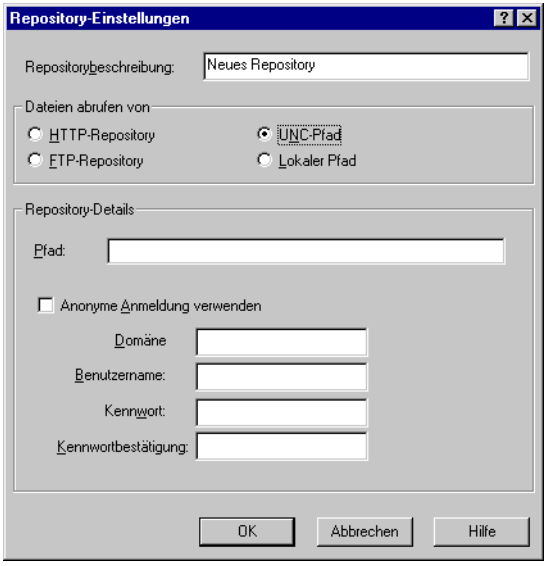


Abbildung 7-7. Repository-Details – UNC-Pfad oder Lokaler Pfad

1 Geben Sie unter **Repository-Details** den Pfad zu dem gewählten Repository ein, und bestimmen Sie, ob Sie das angemeldete Konto verwenden oder durch Angabe von Benutzername und Kennwort die Sicherheit erhöhen möchten. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201.

- **Pfad**: Geben Sie den Pfad zu der Site ein, von der Sie die Aktualisierungsdateien herunterladen möchten.
  - **UNC-Pfad**: Geben Sie entsprechend der UNC-Konvention (\\Servername\Pfad\) den Pfad zu dem Repository ein, in dem sich die Aktualisierungsdateien befinden.
  - **Lokaler Pfad**: Geben Sie den Pfad des lokalen Ordners ein, in dem Sie die Aktualisierungsdateien gespeichert haben, oder klicken Sie auf **Durchsuchen**, um diesen Ordner zu suchen.

    HINWEIS
    Der Pfad kann auf einen Ordner auf einem lokalen Laufwerk oder einem Netzwerklaufwerk verweisen.

- **Angemeldetes Konto verwenden**: Geben Sie das zu verwendende Konto an.
  - Wählen Sie die Option **Angemeldetes Konto verwenden**, um das aktuell angemeldete Konto zu verwenden.
  - Deaktivieren Sie **Angemeldetes Konto verwenden**, um ein anderes Konto verwenden zu können. Geben Sie dazu eine **Domäne**, einen **Benutzernamen**, ein **Kennwort** und unter **Kennwort bestätigen** erneut das Kennwort ein.

    HINWEIS
    Anmeldeinformationen zum Herunterladen sind bei FTP- und UNC-Repositories erforderlich, bei HTTP-Repositories optional. AutoUpdate verwendet die angegebenen Anmeldeinformationen für den Zugriff auf das Repository, so dass die benötigten Aktualisierungsdateien heruntergeladen werden können. Beim Konfigurieren der Anmeldeinformationen für das Konto im Repository müssen Sie darauf achten, dass das Konto *Lese*berechtigungen für die Ordner mit den Aktualisierungsdateien besitzt.

    Bei UNC-Aktualisierungen haben Sie außerdem die Möglichkeit, das angemeldete Konto zu verwenden. Dadurch kann der Aktualisierungs-Task die Berechtigungen der angemeldeten Benutzer zum Zugriff auf das Repository nutzen.

2 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zur Registerkarte **Repositories** zurückzukehren.

Entfernen und Neuorganisieren von Repositories

So können Sie Repositories aus der Repository-Liste entfernen oder neu organisieren:

1 Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.

2 Wählen Sie die Option **Extras** | **AutoUpdate-Repository-Liste bearbeiten**.

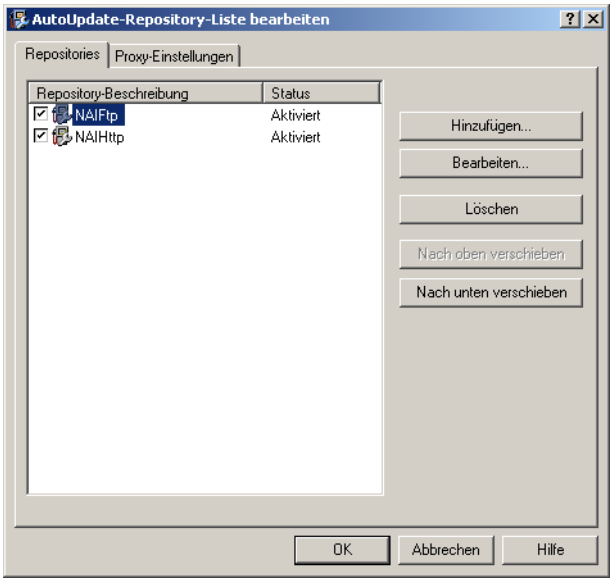


Abbildung 7-8. AutoUpdate-Repository-Liste bearbeiten – Registerkarte "Repositories"

3 Wählen Sie die Registerkarte **Repositories**.

4 Wählen Sie eine der folgenden Optionen aus, um Repositories aus der Repository-Liste zu entfernen oder neu zu organisieren:

- Sie können ein Repository entfernen, indem Sie in der Liste markieren und anschließend auf **Löschen** klicken.
- Um die Repositories in der Liste neu zu organisieren, markieren Sie ein Repository und klicken dann so oft auf **Nach oben** oder **Nach unten**, bis das Repository an der gewünschten Stelle in der Liste steht.

HINWEIS
Die Reihenfolge, in der die Repositories in der Liste aufgeführt werden, entspricht der Reihenfolge, in der sie bei einer Aktualisierung aufgerufen werden.

Festlegen von Proxy-Einstellungen

Proxy-Server werden in der Regel im Rahmen der Internetsicherheit dazu verwendet, die Computer von Internetbenutzern zu maskieren und die Zugriffsgeschwindigkeit durch die Zwischenspeicherung von Sites, auf die häufig zugegriffen wird, zu erhöhen.

Wenn in Ihrem Netzwerk ein Proxy-Server verwendet wird, können Sie die zu verwendenden Proxy-Einstellungen und die Adresse des Proxy-Servers angeben und festlegen, ob die Authentifizierung verwendet werden soll. Proxy-Informationen werden in der AutoUpdate-Repository-Liste (SITELIST.XML) gespeichert. Die hier konfigurierten Proxy-Einstellungen sind für alle Repositories in der Repository-Liste gültig.

So legen Sie die Proxy-Einstellungen fest:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie die Option **Extras** | **AutoUpdate-Repository-Liste bearbeiten**.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen**.

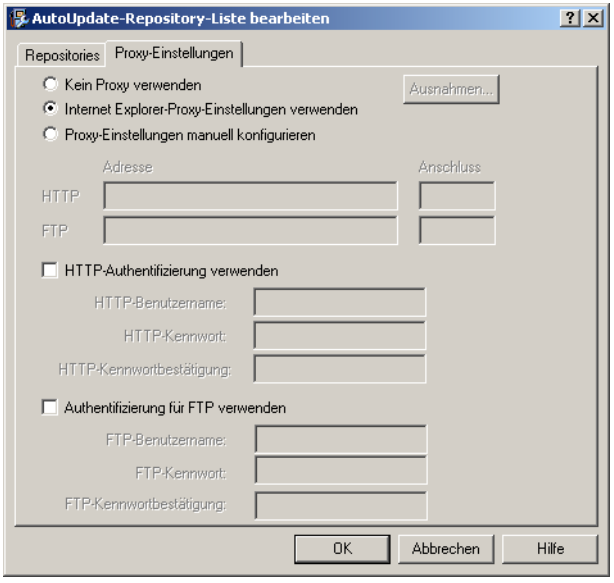


Abbildung 7-9. AutoUpdate-Repository-Liste bearbeiten – Registerkarte "Proxy-Einstellungen"

4 Legen Sie fest, ob Sie einen Proxy verwenden möchten und wenn ja, welche Einstellungen dafür gewählt werden sollen. Wählen Sie eine der folgenden Optionen aus:

- **Keinen Proxy verwenden**: Es wird kein Proxy-Server angegeben. Wählen Sie diese Option und klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** zu schließen.
- **Internet Explorer-Proxy-Einstellungen verwenden**: *Diese Option ist standardmäßig ausgewählt.* Die Proxy-Einstellungen werden für die gegenwärtig installierte Version von Internet Explorer verwendet. Wählen Sie diese Option und klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** zu schließen.
- **Proxy-Einstellungen manuell konfigurieren**: Konfigurieren Sie die Proxy-Einstellungen für Ihre Anforderungen. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201.

  Wählen Sie diese Option und geben Sie dann die Adresse und den Port für das ausgewählte Repository ein:

  - **HTTP-Adresse**: Geben Sie die Adresse des HTTP-Proxy-Servers ein.
  - **HTTP-Port**: Geben Sie die Portnummer des HTTP-Proxy-Servers ein.
  - **FTP-Adresse**: Geben Sie die Adresse des FTP-Proxy-Servers ein.
  - **FTP-Port**: Geben Sie die Portnummer des FTP-Proxy-Servers ein.

  Legen Sie fest, ob für den ausgewählten HTTP- oder FTP-Proxy-Server eine Authentifizierung verwendet werden soll. Wählen Sie eine der folgenden Optionen aus:

  - **Authentifizierung für HTTP verwenden**: Aktivieren Sie diese Option, wenn Sie den HTTP-Proxy-Server mit einer Authentifizierung versehen möchten. Geben Sie dazu einen **HTTP-Benutzernamen** und ein **HTTP-Kennwort** ein, dessen Eingabe Sie unter **HTTP-Bestätigungskennwort** wiederholen.
  - **Authentifizierung für FTP verwenden**: Aktivieren Sie diese Option, wenn Sie den FTP-Proxy-Server mit einer Authentifizierung versehen möchten. Geben Sie dazu einen **FTP-Benutzernamen** und ein **FTP-Kennwort** ein, dessen Eingabe Sie unter **FTP-Bestätigungskennwort** wiederholen.

5 Klicken Sie auf **Ausnahmen**, wenn Sie für die Verwendung des Proxys Ausnahmen festlegen möchten. Wenn keine Ausnahmen festgelegt werden sollen, übergehen Sie diesen Schritt und fahren mit Schritt 6 fort.

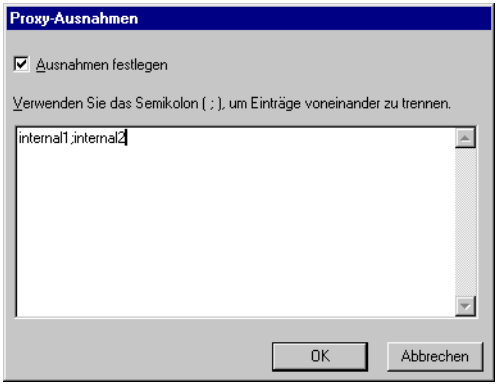


Abbildung 7-10. Proxy-Ausnahmen

a Aktivieren Sie **Ausnahmen angeben** und geben Sie die Ausnahmen durch Semikolons voneinander getrennt ein.

b Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zur Registerkarte **Proxy-Einstellungen** zurückzukehren.

6 Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und das Dialogfeld **AutoUpdate-Repository-Liste bearbeiten** zu schließen.

Spiegelungstasks

Die VirusScan Enterprise-Software vertraut darauf, dass sich die Verzeichnisstruktur selbst aktualisiert. Mit dem Spiegelungstask können Sie Aktualisierungsdateien aus dem ersten erreichbaren Repository, das in der Repository-Liste definiert ist, in eine Spiegelungssite in Ihrem Netzwerk replizieren. Achten Sie darauf, die gesamte Verzeichnisstruktur zu replizieren, wenn Sie eine Site spiegeln. Diese Verzeichnisstruktur unterstützt auch frühere Versionen von VirusScan und NetShield, solange die gesamte Verzeichnisstruktur an die gleichen Speicherorte repliziert wird, die VirusScan 4.5.1 für die Aktualisierung verwendet hat.

Im Folgenden sehen Sie die Verzeichnisstruktur im Repositor, nachdem eine Spiegelungstask verwendet wurde, um das Network Associates-Repository zu replizieren.

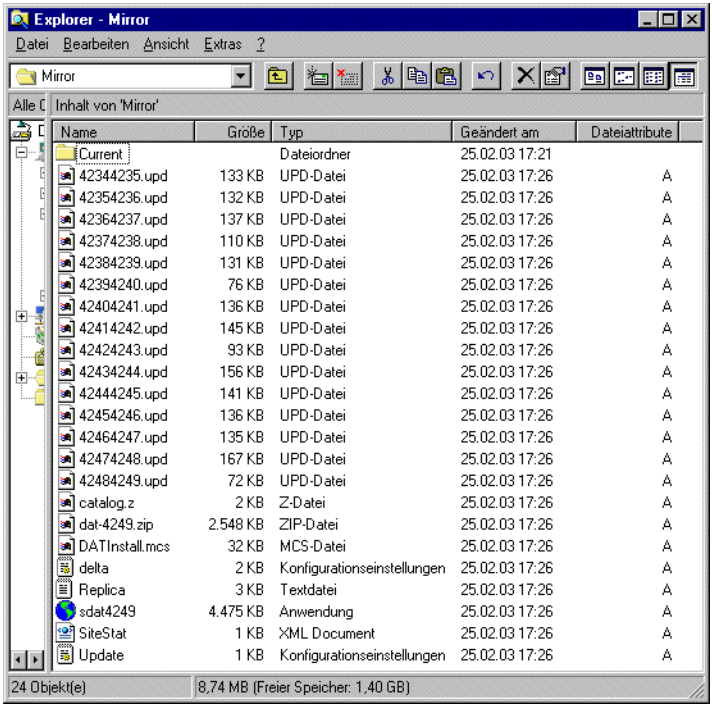

Explorer - Mirror
Datei Bearbeiten Ansicht Extras ?
Mirror
Alle D
Inhalt von 'Mirror'
Name Größe Typ Geändert am Dateiattribute
Current Dateiordner 25.02.03 17:21
42344235.upd 133 KB UPD-Datei 25.02.03 17:26 A
42354236.upd 132 KB UPD-Datei 25.02.03 17:26 A
42364237.upd 137 KB UPD-Datei 25.02.03 17:26 A
42374238.upd 110 KB UPD-Datei 25.02.03 17:26 A
42384239.upd 131 KB UPD-Datei 25.02.03 17:26 A
42394240.upd 76 KB UPD-Datei 25.02.03 17:26 A
42404241.upd 136 KB UPD-Datei 25.02.03 17:26 A
42414242.upd 145 KB UPD-Datei 25.02.03 17:26 A
42424243.upd 93 KB UPD-Datei 25.02.03 17:26 A
42434244.upd 156 KB UPD-Datei 25.02.03 17:26 A
42444245.upd 141 KB UPD-Datei 25.02.03 17:26 A
42454246.upd 136 KB UPD-Datei 25.02.03 17:26 A
42464247.upd 135 KB UPD-Datei 25.02.03 17:26 A
42474248.upd 167 KB UPD-Datei 25.02.03 17:26 A
42484249.upd 72 KB UPD-Datei 25.02.03 17:26 A
catalog.z 2 KB Z-Datei 25.02.03 17:26 A
dat-4249.zip 2.548 KB ZIP-Datei 25.02.03 17:26 A
DATInstall.mcs 32 KB MCS-Datei 25.02.03 17:26 A
delta 2 KB Konfigurationseinstellungen 25.02.03 17:26 A
Replica 3 KB Textdatei 25.02.03 17:26 A
sdat4249 4.475 KB Anwendung 25.02.03 17:26 A
SiteStat 1 KB XML Document 25.02.03 17:26 A
Update 1 KB Konfigurationseinstellungen 25.02.03 17:26 A
24 Objekt(e)
8,74 MB (Freier Speicher: 1,40 GB)

Abbildung 7-11. Gespiegelte Site

Nachdem Sie die Network Associates-Site repliziert haben, die die Aktualisierungsdateien enthält, können Computer in Ihrem Netzwerk die Dateien von der Spiegel-Site herunterladen. Diese Vorgehensweise wird *empfohlen*, da sämtliche Netzwerkcomputer mit oder ohne Internetzugriff aktualisiert werden können, und sie ist *effizient*, da die Computer mit einem Server kommunizieren, der möglicherweise näher als die Network Associates-Internetsite liegt, wodurch der Aufwand und die Zeit zum Herunterladen verringert werden. Dieser Task wird meist zum *Spiegeln* des Inhalts der Network Associates-Downloadsite auf einen lokalen Server verwendet.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Erstellen eines Spiegelungstasks
- Konfigurieren eines Spiegelungstasks
- Ausführen von Spiegelungstasks
- Anzeigen des Aktivitätsprotokolls für Spiegelungstasks

Erstellen eines Spiegelungstasks

Sie können einen Spiegelungstask für jedes benötigte Spiegelverzeichnis erstellen.

So erstellen Sie einen neuen Spiegelungstask:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Erstellen Sie einen neuen Spiegelungstask mithilfe einer der folgenden Methoden:
   - Klicken Sie mit der rechten Maustaste in einen leeren Bereich der Konsole, *ohne ein Element in der Taskliste zu markieren*. Wählen Sie dann **Neuer Spiegelungstask**.
   - Wählen Sie aus dem Menü **Task** die Option **Neuer Spiegelungstask**.

     In der Taskliste der **VirusScan-Konsole** wird ein neuer Spiegelungstask markiert angezeigt.
3. Übernehmen Sie den Standard-Task-Namen oder geben Sie einen neuen Namen für diesen Task ein und drücken Sie dann die EINGABETASTE, um das Dialogfeld **Eigenschaften von VirusScan AutoUpdate** zu öffnen. Ausführliche Konfigurationsinformationen finden Sie unter *Konfigurieren eines Spiegelungstasks* auf Seite 226.

HINWEIS
Wenn Sie Spiegelungstasks über ePolicy Orchestrator 3.0 oder höher erstellen und und Tasksichtbarkeit aktivieren, sind diese Spiegelungstasks in der VirusScan-Konsole sichtbar. Auf diese ePolicy Orchestrator-Tasks besteht nur *Lesezugriff* und sie können nicht von der VirusScan-Konsole aus konfiguriert werden. Weitere Informationen finden Sie im *VirusScan Enterprise Konfigurationshandbuch für die Verwendung mit ePolicy Orchestrator 3.0*.

Konfigurieren eines Spiegelungstasks

Sie können einen Spiegelungstask Ihren Anforderungen entsprechend konfigurieren und planen.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Öffnen Sie das Dialogfeld **Eigenschaften von AutoUpdate**. Verwenden Sie dabei eine der folgenden Vorgehensweisen:
   - Markieren Sie den Task in der Taskliste der Konsole und wählen Sie dann aus dem Menü **Task** die Option **Eigenschaften**.
   - Doppelklicken Sie in der Taskliste auf den Task.
   - Klicken Sie mit der rechten Maustaste in der Taskliste auf den Task, und wählen Sie anschließend **Eigenschaften**.
   - Markieren Sie den Task in der Taskliste und klicken Sie auf  .

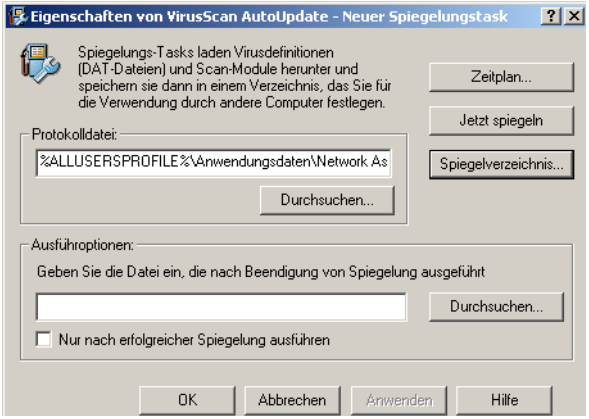


Abbildung 7-12. Eigenschaften von VirusScan AutoUpdate – Neuer Spiegelungstask

HINWEIS
Konfigurieren Sie den Spiegelungstask, bevor Sie auf **Zeitplan** oder **Jetzt aktualisieren** klicken.

3 Sie können den im Textfeld **Protokolldatei** angezeigten Standardnamen und -speicherort der Protokolldatei übernehmen, einen anderen Protokolldateinamen und -speicherort eingeben oder auf **Durchsuchen** klicken, um zu einem anderen geeigneten Speicherort zu wechseln. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201.

HINWEIS
Standardmäßig werden Protokollinformationen in die Datei VSEMIRRORLOG.TXT in diesem Ordner geschrieben:

```
<Laufwerk>:Winnt\Profiles\All Users\Application
Data\Network Associates\VirusScan
```

4 Klicken Sie auf **Spiegelverzeichnis**, um das Dialogfeld **Einstellungen für das Spiegelverzeichnis** zu öffnen.

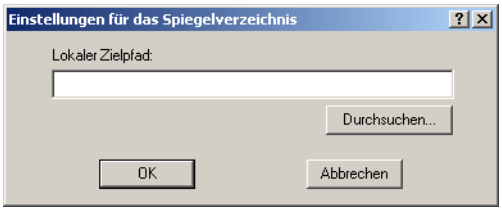


Abbildung 7-13. Einstellungen für das Spiegelverzeichnis

a Geben Sie den Pfad zu dem Zielverzeichnis auf dem lokalen System ein, das Sie für die Spiegelsite verwenden, oder klicken Sie auf **Durchsuchen**, um zu dem gewünschten Speicherort zu navigieren. Systemvariablen werden unterstützt. Weitere Informationen finden Sie unter *Systemvariablen* auf Seite 201.

b Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften von VirusScan AutoUpdate** zurückzukehren.

5 Unter **Ausführoptionen** können Sie eine ausführbare Datei angeben, die ausgeführt wird, nachdem der **Spiegelungstask** abgeschlossen ist. Sie können mit dieser Option z. B. ein Dienstprogramm für Netzwerkmeldungen starten, so dass der Administrator benachrichtigt wird, dass der Aktualisierungsvorgang erfolgreich abgeschlossen wurde.

- **Geben Sie die ausführbare Datei an, die nach Abschluss des Spiegelungstasks ausgeführt werden soll**. Geben Sie den Pfad zu der auszuführenden Datei ein oder klicken Sie auf **Durchsuchen**, um nach der Datei zu suchen.

- **Nur nach erfolgreichen Spiegelungen ausführen**. Das ausführbare Programm wird nur nach einer erfolgreichen Aktualisierung ausgeführt. Wenn die Aktualisierung jedoch fehlschlägt, wird die ausgewählte Programmdatei nicht ausgeführt.

  HINWEIS
  Die angegebene Programmdatei muss vom derzeit angemeldeten Benutzer ausgeführt werden können. Wenn der derzeit angemeldete Benutzer über keine Zugriffsrechte auf das Verzeichnis mit den Programmdateien verfügt bzw. wenn zur Zeit keine Benutzer angemeldet sind, wird das Programm nicht ausgeführt.

6. Klicken Sie auf **Zeitplan**, um den Spiegelungstask zu planen. Weitere Informationen zum Planen von Tasks finden Sie unter *Planen von Tasks* auf Seite 235.
7. Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.
8. Wenn Sie den Spiegelungstask sofort ausführen möchten, klicken Sie auf **Jetzt spiegeln**.
9. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften von VirusScan AutoUpdate** zu schließen.

   HINWEIS
   Der **Spiegelungstask** verwendet die Konfigurationseinstellungen in der Repository-Liste, um die Aktualisierung auszuführen. Weitere Informationen finden Sie unter *AutoUpdate-Repository-Liste* auf Seite 210.

Ausführen von Spiegelungstasks

Nachdem Sie den Spiegelungstask mit den gewünschten Eigenschaften konfiguriert haben, können Sie ihm mithilfe einer der folgenden Methoden ausführen:

- **Spiegeln nach Zeitplan**: Wenn der Spiegelungstask geplant wurde, können Sie den Task unbeaufsichtigt ausführen lassen.

  HINWEIS
  Der Computer muss zum Ausführen des Spiegelungstasks eingeschaltet sein. Wenn der Computer zum Zeitpunkt der geplanten Ausführung des Tasks heruntergefahren ist, wird der Task entweder zum nächsten geplanten Zeitpunkt gestartet, zu dem der Computer eingeschaltet ist, oder wenn der Computer neu gestartet wird. Hierfür muss jedoch auf der Registerkarte **Zeitplan** unter **Zeitplaneinstellungen** die Option **Ausgelassenen Task ausführen** aktiviert sein.

- **Sofortiges Spiegeln**: Zum sofortigen Starten von Spiegelungstasks stehen Ihnen zwei Methoden zur Verfügung:
  - **Start**-Befehl für Spiegelungstasks
  - Befehl **Jetzt spiegeln** für Spiegelungstasks

Start-Befehl für Spiegelungstasks

Verwenden Sie in der **VirusScan-Konsole** die Option **Starten**, um alle Spiegelungstasks sofort zu starten.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Um einen sofortigen Spiegelungstask über die **VirusScan-Konsole** zu starten, verwenden Sie eine der folgenden Vorgehensweisen:
   - Markieren Sie den Task in der Taskliste der Konsole und wählen Sie dann aus dem Menü **Task** die Option **Starten**.
   - Klicken Sie mit der rechten Maustaste in der Taskliste auf den Task und wählen Sie anschließend **Starten**.
   - Markieren Sie den Task in der Taskliste und klicken Sie auf  .
   - Wenn der Task abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee Updater** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

Befehl "Jetzt spiegeln" für Spiegelungstasks

Verwenden Sie im Dialogfeld **Eigenschaften von VirusScan AutoUpdate** die Option **Jetzt spiegeln**, um alle Spiegelungstasks sofort zu starten.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Öffnen Sie für den ausgewählten Spiegelungstask das Dialogfeld **Eigenschaften von VirusScan AutoUpdate**. Anleitungen finden Sie unter *Konfigurieren eines Spiegelungstasks* auf Seite 226.
3. Klicken Sie im Dialogfeld **Eigenschaften von VirusScan AutoUpdate** auf **Jetzt spiegeln**.
4. Wenn der Task abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee Updater** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

Anzeigen des Aktivitätsprotokolls für Spiegelungstasks

Das Aktivitätsprotokoll für Spiegelungstasks zeigt spezifische Details zum Aktualisierungsvorgang an. So werden z. B. die Versionsnummern der aktualisierten DAT-Datei und des Scan-Moduls angezeigt.

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Öffnen Sie die Aktivitätsprotokolldatei mit einer der folgenden Methoden**:**
   - Markieren Sie den Task und wählen Sie dann im Menü **Task** die Option **Aktivitätsprotokoll**.
   - Klicken Sie mit der rechten Maustaste auf den Task in der Taskliste und wählen Sie die Option **Protokoll anzeigen**.
3. Wählen Sie zum Schließen des Aktivitätsprotokolls aus dem Menü **Datei** die Option **Beenden**.

Rollback für DAT-Dateien

Mit dieser Funktion können Sie die DAT-Dateien auf die letzte gesicherte Version zurückführen, wenn die aktuellen DAT-Dateien aus einem bestimmten Grund beschädigt oder inkompatibel sein sollten. Wenn Sie DAT-Dateien aktualisieren, wird die alte Version in diesem Verzeichnis gespeichert:

```
C:\Programme\Gemeinsame Dateien\Network Associates\Engine\OldDats
```

Wenn Sie ein Rollback der DAT-Dateien durchführen, werden die aktuellen DAT-Dateien mit der Version im Ordner *OldDats* ersetzt und in der Registrierung wird an dieser Stelle ein Flag gesetzt:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\TVD\VirusScan
Enterprise\CurrentVersion\szRollbackedDATS
```

Nach dem Rollback ist eine Rückkehr zu der vorhergehenden Version nicht möglich. Bei der nächsten Aktualisierung wird die DAT-Version in der Registrierung mit den DAT-Dateien im Aktualisierungs-Repository verglichen. Wenn die neuen DAT-Dateien mit der in der Registrierung durch Flag gekennzeichneten Version übereinstimmen, wird keine Aktualisierung ausgeführt.

So führen Sie ein Rollback der DAT-Dateien durch:

1. Öffnen Sie die **VirusScan-Konsole**. Anweisungen dazu finden Sie unter *VirusScan-Konsole* auf Seite 23.
2. Wählen Sie die Option **Extras** | **Rollback für DATs durchführen**. Das Dialogfeld **McAfee Updater** wird aufgerufen.

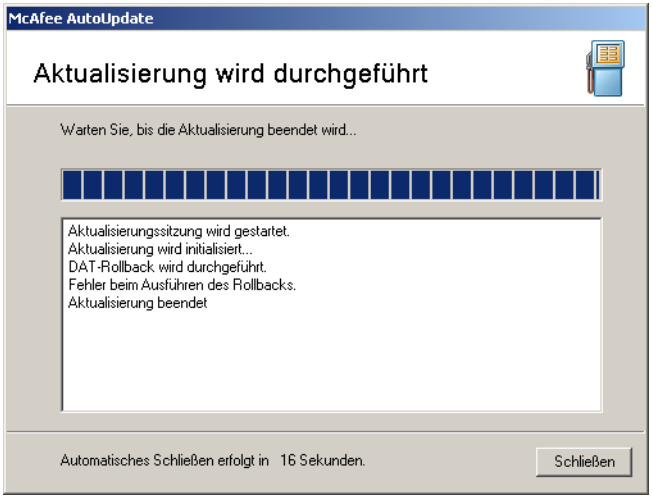


Abbildung 7-14. Rollback für DATs durchführen – Aktualisierung wird durchgeführt

3 Ein Rollback ist mit einer Aktualisierung vergleichbar, mit der Ausnahme, dass in den Details DAT-*Rollback wird durchgeführt* angezeigt wird. Wenn der Rollback abgeschlossen ist, klicken Sie auf **Schließen**, um das Dialogfeld **McAfee AutoUpdate** zu schließen, oder warten Sie, bis das Fenster automatisch geschlossen wird.

HINWEIS
Beim Ausführen eines Rollbacks wird die letzte Sicherung der DAT-Dateien wiederhergestellt.

Manuelle Aktualisierungen

McAfee Security empfiehlt, zur Installation neuer Versionen der DAT-Dateien oder Scan-Modul-Versionen den im Lieferumfang der Software VirusScan Enterprise enthaltenen AutoUpdate-Task zu verwenden. Mit diesem Dienstprogramm ist die fehlerfreie Aktualisierung der DAT-Dateien und des Scan-Moduls ebenso einfach wie sicher. Wenn Sie die DAT-Dateien selbst installieren möchten, können Sie die DAT-Dateien manuell von diesen Update-Standorten herunterladen:

http:www.networkassociates.com/us/downloads/updates

ftp://ftp.nai.com/CommonUpdater

- **Reguläre DAT-Dateien**: Diese Dateien sind auf der FTP-Site von McAfee Security als .ZIP-Archive mit der Bezeichnung DAT-XXXX.ZIP gespeichert. Die Zeichenfolge XXXX im Dateinamen steht für eine Seriennummer, die sich mit jeder DAT-Dateiversion ändert. Zum Herunterladen dieser Dateien verwenden Sie einen Webbrowser oder FTP-Client und stellen eine Verbindung zu der folgenden Adresse her:

  ftp://ftp.nai.com/CommonUpdater

- **Installierbare .EXE-Dateien**: Diese Dateien werden auf der Website von McAfee Security als ausführbare Setup-Datei mit der Bezeichnung XXXXUPDT.EXE gespeichert. Auch hier steht die Zeichenfolge XXXX im Dateinamen für eine Seriennummer, die sich mit jeder neuen DAT-Version ändert. Zum Herunterladen dieser Dateien verwenden Sie einen Webbrowser und stellen eine Verbindung zu der folgenden Adresse her:

  http:www.networkassociates.com/us/downloads/updates

  Die DAT-Dateien in den beiden Dateien sind identisch. Ein Unterschied besteht lediglich darin, wie Sie sie verwenden, um Ihre Kopie der VirusScan Enterprise-Software zu aktualisieren.

Zur Verwendung des DAT-XXXX.ZIP-Archivs müssen Sie die Datei herunterladen und aus dem Archiv extrahieren. Anschließend werden die Dateien in den DAT-Ordner kopiert und der Zugriffsscanner wird neu gestartet. Eine ausführlichere Anleitung finden Sie unter *Aktualisieren über DAT-Dateiarchive* auf Seite 233.

Zur Installation der DAT-Dateien, die ein eigenes Setup-Programm besitzen, müssen Sie diese Dateien lediglich in einen temporären Ordner auf der Festplatte herunterladen und anschließend die Datei XXXUPDT.EXE ausführen, indem Sie darauf doppelklicken. Das Setup-Programm hält den Zugriffsscanner an, kopiert die Dateien in den entsprechenden Ordner und startet den Scanner dann neu.

HINWEIS
Zum Schreiben in den DAT-Ordner benötigen Sie Administratorrechte.

Nach der Aktualisierung greifen der Zugriffsscanner, der Anforderungsscanner und der E-Mail-Scanner beim nächsten Scanner-Start auf die DAT-Dateien zu.

Aktualisieren über DAT-Dateiarchive

So können Sie DAT-Dateiaktualisierungen direkt aus einem .ZIP-Archiv installieren, *ohne* dabei AutoUpdate zu verwenden:

1. Erstellen Sie einen temporären Ordner auf der Festplatte. Kopieren Sie das heruntergeladene ZIP-Archiv mit den .DAT-Dateien in diesen Ordner.
2. Erstellen Sie eine Sicherungskopie der DAT-Dateien oder benennen Sie sie um.
   - CLEAN.DAT
   - NAMES.DAT
   - SCAN.DAT

   Wenn Sie den standardmäßigen Installationspfad übernommen haben, werden die Dateien unter dem folgenden Pfad abgelegt:

   ```
   Laufwerk:\Programme\Gemeinsame Dateien\Network Associates\Engine
   ```
3. Verwenden Sie WINZIP, PKUNZIP oder ein vergleichbares Dienstprogramm, um das .ZIP-Archiv zu öffnen und die aktualisierten DAT-Dateien zu extrahieren.
4. Melden Sie sich bei dem Server an, der aktualisiert werden soll. Für den Zielcomputer benötigen Sie Administratorrechte.
5. Kopieren Sie die DAT-Dateien in den DAT-Ordner.
6. Deaktivieren Sie das Scannen bei Zugriff durch Stoppen des McShield-Dienstes und aktivieren Sie es dann erneut, indem Sie den McShield-Dienst starten.
7. Beenden Sie Microsoft Outlook und starten Sie es danach erneut.
8. Beenden Sie die Anforderungsscan-Tasks und starten Sie sie danach erneut.

Planen von Tasks 8

Sie können VirusScan Enterprise-Tasks so planen, dass sie an bestimmten Tagen, zu bestimmten Zeiten oder in bestimmten Abständen durchgeführt werden. Zeitpläne können ganz auf die Anforderungen Ihres Unternehmens abgestimmt werden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Task-Pläne konfigurieren

Task-Pläne konfigurieren

Sie können drei Typen von Tasks planen:

- Anforderungstasks: Um einen Anforderungstask zu planen, öffnen Sie die **Eigenschaften für das Scannen auf Anforderung** für den Task und klicken auf **Zeitplan**. Das Dialogfeld **Zeitplaneinstellungen** wird aufgerufen.

  Weitere Informationen zum Planen von Anforderungstasks finden Sie unter *Scannen auf Anforderung* auf Seite 95.

- AutoUpdate-Tasks: Zum Planen eines AutoUpdate-Tasks öffnen Sie die **AutoUpdate-Eigenschaften** für den AutoUpdate-Task und klicken auf **Zeitplan**. Das Dialogfeld **Zeitplaneinstellungen** wird aufgerufen.

  Weitere Informationen zu AutoUpdate-Tasks finden Sie unter *AutoUpdate-Tasks* auf Seite 202.

- Spiegelungstasks: Zum Planen eines Spiegelungstasks öffnen Sie die **AutoUpdate-Eigenschaften** für den Spiegelungstask und klicken auf **Zeitplan**. Das Dialogfeld **Zeitplaneinstellungen** wird aufgerufen.

  Weitere Informationen über Spiegelungstasks finden Sie unter *Spiegelungstasks* auf Seite 224.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Task-Eigenschaften
- Eigenschaften des Zeitplans

Task-Eigenschaften

Verwenden Sie die Optionen auf der Registerkarte **Task**, um die Zeitplanung zu aktivieren, und geben Sie eine Grenze für die Ausführungszeit sowie die Authentifizierungsdaten für den Task an.

1 Wählen Sie die Registerkarte **Task**.



Abbildung 8-1. Zeitplaneinstellungen – Registerkarte "Task"

2 Geben Sie unter **Zeitplaneinstellungen** an, ob der Task zu einer bestimmten Zeit ausgeführt werden soll. Sie haben folgende Optionen:

- **Aktivieren (geplanter Task wird zur festgesetzten Zeit ausgeführt)**: Die Ausführung des Tasks wird für eine bestimmte Zeit geplant.
- **Task stoppen nach**: Der Task wird nach einer begrenzten Zeit gestoppt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** eingeben bzw. auswählen.

  HINWEIS
  Wenn der Task abgebrochen wird, bevor er abgeschlossen ist, wird der Scan-Vorgang bei einem erneuten Start an der Stelle der Unterbrechung wieder aufgenommen, es sei denn, die DAT-Dateien wurden aktualisiert und Sie haben die Option **Alle Dateien beim Aktualisieren von DAT-Dateien erneut scannen** aktiviert. In diesem Fall wird der Scan-Vorgang nicht fortgesetzt, sondern von Anfang an ausgeführt.

3 Geben Sie unter **Task** die folgenden Authentifizierungsdaten für den Task ein:

HINWEIS
Die Verwendung von Anmeldedaten ist optional. Wenn Sie hier keine Anmeldedaten eingeben, wird der geplante Task unter dem lokalen Systemkonto ausgeführt.

- **Benutzer**: Geben Sie die Benutzer-ID ein, unter der der Task ausgeführt wird.
- **Domäne**: Geben Sie die Domäne für die angegebene Benutzer-ID ein.
- **Kennwort**: Geben Sie das Kennwort für die angegebene Benutzer-ID ein.

4 Klicken Sie auf **Anwenden**, um Ihre Änderungen zu speichern.

HINWEIS
Wenn Sie einen Task mit Anmeldedaten planen, muss für das angegebene Konto die Berechtigung *Anmelden als Stapelverarbeitungsauftrag* aktiviert sein. Ohne diese Berechtigung kann der eingeleitete Prozess nicht auf Netzwerkressourcen zugreifen, selbst wenn die richtigen Anmeldeinformationen vorhanden sind. Dieses Verhalten ist in Windows NT dokumentiert.

So weisen Sie einem Konto diese Berechtigung zu:

- **Start** | **Programme** | **Verwaltung** | **Lokale Sicherheitsrichtlinie**.
- **Sicherheitseinstellungen** | **Lokale Richtlinien** | **Zuweisen von Benutzerrechten**.
- Doppelklicken Sie auf **Anmelden als Stapelverarbeitungsauftrag**.
- Fügen Sie der Liste den Benutzer hinzu.
- Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Eigenschaften des Zeitplans

Mit den Optionen auf der Registerkarte **Zeitplan** können Sie angeben, wie oft der Task ausgeführt werden soll, ob der Task in verschiedenen Zeitzonen ausgeführt wird, ob er zu zufällig ausgewählten Zeiten innerhalb eines bestimmten Intervalls ausgeführt wird oder ob ausgelassene Tasks ausgeführt werden sollen, und Sie können die Verzögerungszeiten für ausgelassene Tasks festlegen.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Planen der Häufigkeit von Tasks
- Erweiterte Zeitplanoptionen
- Planen von Tasks nach Häufigkeit

Planen der Häufigkeit von Tasks

Der hier ausgewählte Wert wirkt sich auf die Optionen aus, mit denen Sie für den Zeitplan Tage, Wochen, Monate und andere Häufigkeitsangaben auswählen können. Folgende Häufigkeitsoptionen stehen zur Auswahl:

- **Täglich***Diese Option ist standardmäßig ausgewählt.* Der Task wird an den festgelegten Tagen täglich ausgeführt. Siehe *Täglich* auf Seite 241.
- **Wöchentlich**: Der Task wird in den festgelegten Wochen an den festgelegten Tagen wöchentlich ausgeführt. Siehe *Wöchentlich* auf Seite 243.
- **Monatlich**: Der Task wird in den festgelegten Monaten an den festgelegten Tagen monatlich ausgeführt. Siehe *Monatlich* auf Seite 244.
- **Einmal**: Der Task wird am festgelegten Termin einmal ausgeführt. Siehe *Einmal* auf Seite 246.
- **Bei Systemstart**: Der Task wird beim Systemstart ausgeführt. Geben Sie darüber hinaus an, ob der Task einmal am Tag ausgeführt werden soll und um wie viele Minuten der Task verzögert werden soll. Siehe *Bei Systemstart* auf Seite 248.
- **Bei der Anmeldung**: Der Task wird bei der Anmeldung ausgeführt. Geben Sie darüber hinaus an, ob der Task einmal am Tag ausgeführt werden soll und um wie viele Minuten der Task verzögert werden soll. Siehe *Bei der Anmeldung* auf Seite 249.
- **Bei Leerlauf**: Der Task wird ausgeführt, wenn der Computer im Leerlauf ist. Geben Sie auch die Anzahl der Minuten an. Siehe *Bei Leerlauf* auf Seite 250.
- **Sofort ausführen**: Der Task wird sofort ausgeführt. Siehe *Sofort ausführen* auf Seite 251.
- **Beim Einwählen ausführen**: Der Task wird beim Einwählen ausgeführt. Geben Sie an, ob der Task einmal am Tag ausgeführt werden soll. Siehe *Beim Einwählen ausführen* auf Seite 252.

Erweiterte Zeitplanoptionen

1 Klicken Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** auf **Erweitert**, um das Dialogfeld **Erweiterte Zeitplanoptionen** zu öffnen.



Abbildung 8-2. Erweiterte Zeitplanoptionen

- **Startdatum**: Klicken Sie auf , um ein Datum aus dem Kalender auszuwählen. Dieses Feld ist optional.
- **Enddatum**: Klicken Sie auf , um ein Datum aus dem Kalender auszuwählen. Dieses Feld ist optional.
- **Task wiederholen**: Der Task wird mit der angegebenen Häufigkeit wiederholt.
- **Alle**: Geben Sie die Häufigkeit ein oder verwenden Sie zum Auswählen eines Werts die Pfeile. Geben Sie anschließend an, ob sich der Häufigkeitswert auf Minuten oder Stunden bezieht.
- **Bis**: Wählen Sie entweder **Uhrzeit (Lokal)** und geben Sie die Zeit ein bzw. wählen Sie sie aus oder wählen Sie **Dauer** und geben Sie die **Stunde(n)** und **Minute(n)** ein bzw. wählen Sie sie aus.

2 Klicken Sie auf **OK**, um zur Registerkarte **Zeitplan** zurückzukehren.

Planen von Tasks nach Häufigkeit

Sie können die Ausführung eines Tasks je nach Ihren Anforderungen für ein bestimmtes Datum und/oder für eine bestimmte Zeitspanne planen.

In diesem Abschnitt werden die folgenden Optionen für die Häufigkeit der Task-Ausführung behandelt:

- Täglich
- Wöchentlich
- Monatlich
- Einmal
- Bei Systemstart
- Bei der Anmeldung
- Bei Leerlauf
- Sofort ausführen
- Beim Einwählen ausführen

Täglich

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf ▼, um die Option **Täglich** auszuwählen.

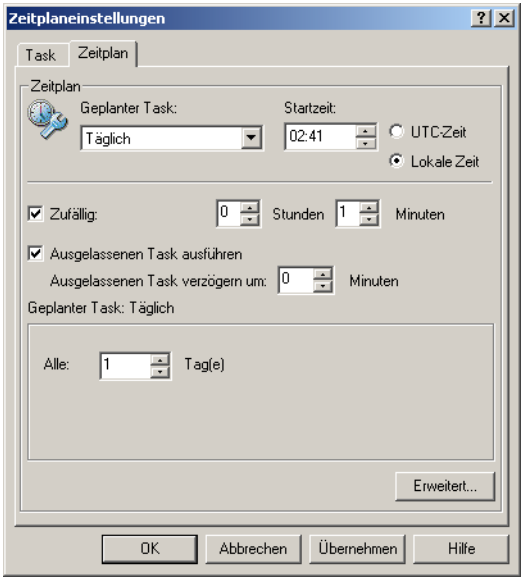


Abbildung 8-3. Registerkarte "Zeitplan" – Täglich

- **Startzeit**: Geben Sie eine Startzeit für den geplanten Task ein oder wählen Sie mit den Pfeilen eine Zeit aus.
- **UTC-Zeit**: Universal Time Coordinated (UTC). Wählen Sie diese Option, wenn der Task gleichzeitig in allen Zeitzonen ausgeführt werden soll.
- **Lokale Zeit**: *Diese Option ist standardmäßig ausgewählt.* Der Task wird in jeder lokalen Zeitzone separat ausgeführt.
- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** für die maximale Zeitspanne eingeben bzw. auswählen.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben bzw. auswählen. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.
- **Ausgelassenen Task ausführen**: Stellt sicher, dass ausgelassene Tasks beim erneuten Starten des Computers ausgeführt werden. Tasks können ausgelassen werden, wenn der Computer zu dem für die Ausführung eines Tasks festgelegten Zeitpunkt offline ist. Mit dieser Funktion wird sichergestellt, dass Remotebenutzer und das Netzwerk umfassend geschützt sind, falls sie bei geplanter Ausführung eines Tasks offline sind.
- **Ausgelassenen Task verzögern um**: Geben Sie die Anzahl der Minuten ein, um die der ausgelassene Task verzögert werden soll, oder wählen Sie mit den Pfeilen einen Wert aus. Sie können einen Wert von 0 bis 99 Minuten auswählen.
- **Erweitert**: Klicken Sie auf diese Schaltfläche, um die erweiterten Zeitplaneigenschaften einzurichten. Weitere Informationen finden Sie unter *Erweiterte Zeitplanoptionen* auf Seite 240.

2 Geben Sie unter **Task täglich planen** die Häufigkeit als Anzahl von Tagen ein bzw. wählen Sie sie aus oder wählen Sie den Wert mithilfe der Pfeile.

> **HINWEIS**
> Täglich ausgeführte Tasks können an beliebig vielen Tagen oder jeden Tag zwischen Montag und Sonntag ausgeführt werden. Wenn Sie einen Task nur an bestimmten Wochentagen ausführen möchten, sollten Sie die Task-Häufigkeit "Wöchentlich" verwenden.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Wöchentlich

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Wöchentlich** auszuwählen.

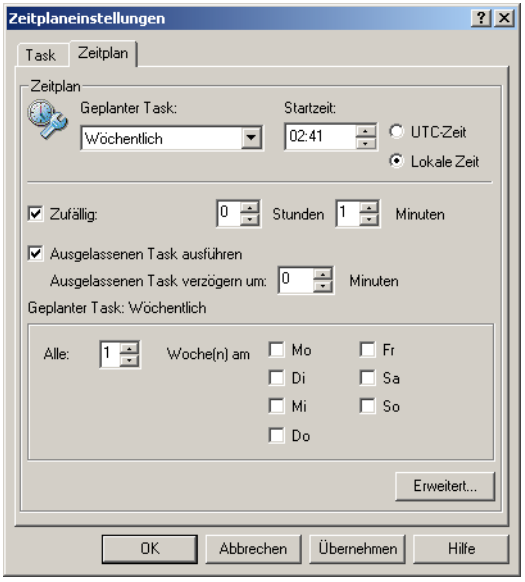


Abbildung 8-4. Registerkarte "Zeitplan" – Wöchentlich

- **Startzeit**: Geben Sie eine Startzeit für den geplanten Task ein oder wählen Sie mit den Pfeilen eine Zeit aus.
- **UTC-Zeit**: Universal Time Coordinated (UTC). Wählen Sie diese Option, wenn der Task gleichzeitig in allen Zeitzonen ausgeführt werden soll.
- **Lokale Zeit**: *Diese Option ist standardmäßig ausgewählt.* Der Task wird in jeder lokalen Zeitzone separat ausgeführt.
- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** für die maximale Zeitspanne eingeben bzw. auswählen.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.

- **Ausgelassenen Task ausführen**: Stellt sicher, dass ausgelassene Tasks beim erneuten Starten des Computers ausgeführt werden. Tasks können ausgelassen werden, wenn der Computer zu dem für die Ausführung eines Tasks festgelegten Zeitpunkt offline ist. Mit dieser Funktion wird sichergestellt, dass Remotebenutzer und das Netzwerk umfassend geschützt sind, falls sie bei geplanter Ausführung eines Tasks offline sind.
- **Ausgelassenen Task verzögern um**: Geben Sie die Anzahl der Minuten ein, um die der ausgelassene Task verzögert werden soll, oder wählen Sie mit den Pfeilen einen Wert aus. Sie können einen Wert von 0 bis 99 Minuten auswählen.
- **Erweitert**: Klicken Sie auf diese Schaltfläche, um die erweiterten Zeitplaneigenschaften einzurichten. Weitere Informationen finden Sie unter *Erweiterte Zeitplanoptionen* auf Seite 240.

2 Gehen Sie unter **Wöchentlichen Task planen** folgendermaßen vor:

- **Alle**: Geben Sie die Häufigkeit als Anzahl der Wochen ein.
- **Woche(n) am**: Wählen Sie die Wochentage aus.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Monatlich

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Monatlich** zu wählen.

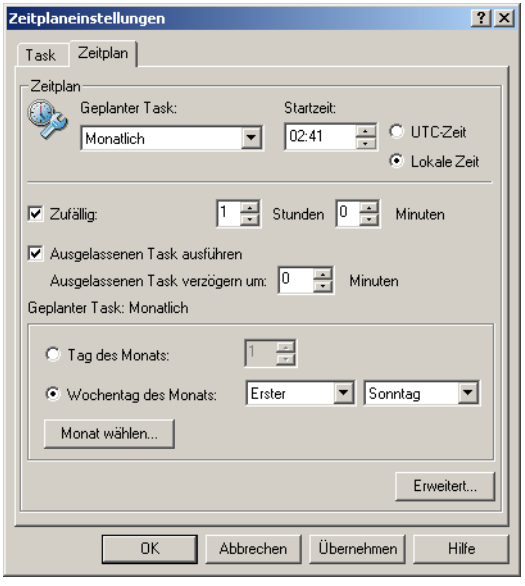


Abbildung 8-5. Registerkarte "Zeitplan" – Monatlich

- **Startzeit**: Geben Sie eine Startzeit für den geplanten Task ein oder wählen Sie mit den Pfeilen eine Zeit aus.
- **UTC-Zeit**: Universal Time Coordinated (UTC). Wählen Sie diese Option, wenn der Task gleichzeitig in allen Zeitzonen ausgeführt werden soll.
- **Lokale Zeit**: *Diese Option ist standardmäßig ausgewählt.* Der Task wird in jeder lokalen Zeitzone separat ausgeführt.
- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen auch **Stunden** und **Minuten** für die maximale Zeitspanne eingegeben werden.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.
- **Ausgelassenen Task ausführen**: Stellt sicher, dass ausgelassene Tasks beim erneuten Starten des Computers ausgeführt werden. Tasks können ausgelassen werden, wenn der Computer zu dem für die Ausführung eines Tasks festgelegten Zeitpunkt offline ist. Mit dieser Funktion wird sichergestellt, dass Remotebenutzer und das Netzwerk umfassend geschützt sind, falls sie bei geplanter Ausführung eines Tasks offline sind.
- **Ausgelassenen Task verzögern um**: Geben Sie die Anzahl der Minuten ein, um die der ausgelassene Task verzögert werden soll, oder wählen Sie mit den Pfeilen einen Wert aus. Sie können einen Wert von 0 bis 99 Minuten auswählen.
- **Erweitert**: Klicken Sie auf diese Schaltfläche, um die erweiterten Zeitplaneigenschaften einzurichten. Weitere Informationen finden Sie unter *Erweiterte Zeitplanoptionen* auf Seite 240.

2 Wählen Sie unter **Task monatlich planen** die entsprechenden Optionen aus:

- **Tag des Monats**: Aktivieren Sie die Option und wählen Sie das Datum des Tages.
- **Wochentag des Monats**: Wählen Sie diese Option, um den Task an einem bestimmten Tag des Monats (z. B. am ersten Sonntag, zweiten Mittwoch usw.) auszuführen.
  - Wählen Sie die Option **Erster**, **Zweiter**, **Dritter**, **Vierter** oder **Letzter**.
  - Wählen Sie den Wochentag aus, an dem dieser Task jeden Monat ausgeführt werden soll.

- Klicken Sie auf **Monate auswählen**, um bestimmte Monate auszuwählen:
  - Wählen Sie die Monate aus, in denen der Task ausgeführt werden soll.

    HINWEIS
    Standardmäßig sind alle Monate ausgewählt.
  - Klicken Sie auf **OK**, um zur Registerkarte **Zeitplan** zurückzukehren.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Einmal

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Einmal** auszuwählen.

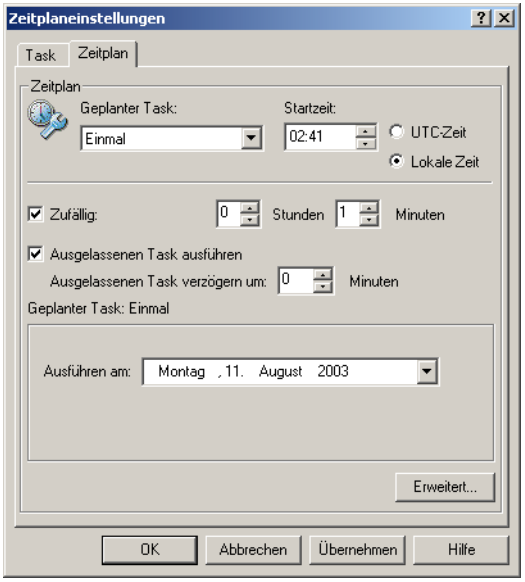


Abbildung 8-6. Registerkarte "Zeitplan" – Einmal

- **Startzeit**: Geben Sie eine Startzeit für den geplanten Task ein oder wählen Sie mit den Pfeilen eine Zeit aus.
- **UTC-Zeit**: Universal Time Coordinated (UTC). Wählen Sie diese Option, wenn der Task gleichzeitig in allen Zeitzonen ausgeführt werden soll.
- **Lokale Zeit**: *Diese Option ist standardmäßig ausgewählt.* Der Task wird in jeder lokalen Zeitzone separat ausgeführt.

- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** für die maximale Zeitspanne eingeben bzw. auswählen.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben bzw. auswählen. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.

- **Ausgelassenen Task ausführen**: Stellt sicher, dass ausgelassene Tasks beim erneuten Starten des Computers ausgeführt werden. Tasks können ausgelassen werden, wenn der Computer zu dem für die Ausführung eines Tasks festgelegten Zeitpunkt offline ist. Mit dieser Funktion wird sichergestellt, dass Remotebenutzer und das Netzwerk umfassend geschützt sind, falls sie bei geplanter Ausführung eines Tasks offline sind.

- **Ausgelassenen Task verzögern um**: Geben Sie die Anzahl der Minuten ein, um die der ausgelassene Task verzögert werden soll, oder wählen Sie mit den Pfeilen einen Wert aus. Sie können einen Wert von 0 bis 99 Minuten auswählen.

- **Erweitert**: Klicken Sie auf diese Schaltfläche, um die erweiterten Zeitplaneigenschaften einzurichten. Weitere Informationen finden Sie unter *Erweiterte Zeitplanoptionen* auf Seite 240.

2. Klicken Sie unter **Task einmal planen** auf  , um das Datum auszuwählen, an dem der Task ausgeführt werden soll.

3. Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Bei Systemstart

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Bei Systemstart** auszuwählen.

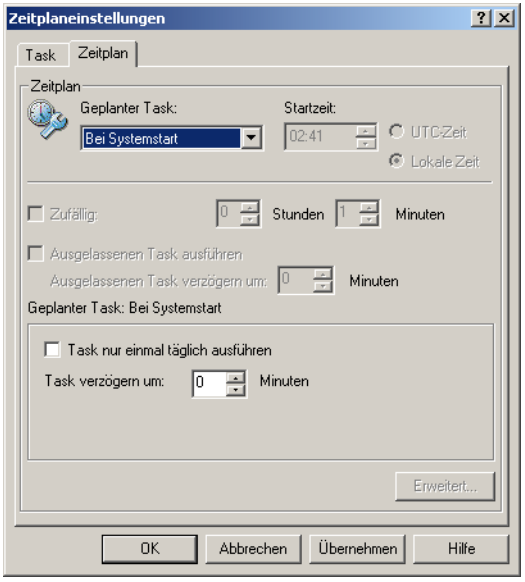


Abbildung 8-7. Registerkarte "Zeitplan" – Bei Systemstart

2 Gehen Sie unter **Task bei Systemstart planen** folgendermaßen vor:

- **Task nur einmal täglich ausführen**: Wählen Sie diese Option, um diesen Task einmal am Tag auszuführen. Wenn Sie diese Option nicht wählen, wird der Task bei jedem Systemstart ausgeführt.
- **Task verzögern um**: Wählen Sie aus, um wie viele Minuten der Task verzögert werden soll. Sie können einen Wert von 0 bis 99 Minuten auswählen. In dieser Zeitspanne können Anmeldeskripte ausgeführt werden oder die Benutzer können sich anmelden.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Bei der Anmeldung

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Bei der Anmeldung** auszuwählen.

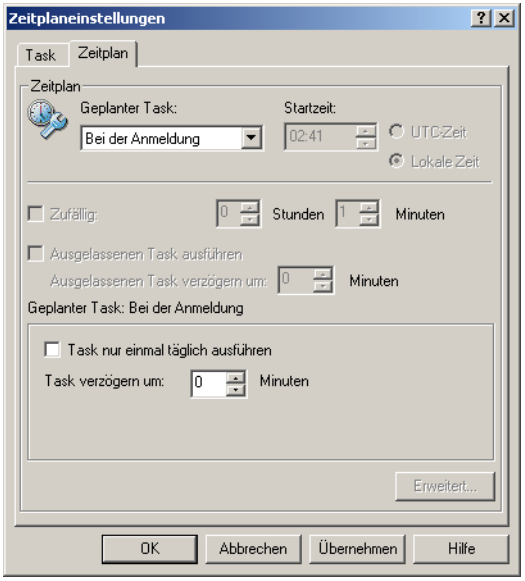


Abbildung 8-8. Registerkarte "Zeitplan" – Bei der Anmeldung

2 Gehen Sie unter **Task bei Anmeldung planen** folgendermaßen vor:

- **Task nur einmal täglich ausführen**: Wählen Sie diese Option, um diesen Task einmal am Tag auszuführen. Wenn Sie diese Option nicht wählen, wird der Task bei jeder Anmeldung ausgeführt.

- **Task verzögern um**: Geben Sie an, um wie viele Minuten der Task verzögert werden soll. Sie können einen Wert von 0 bis 99 Minuten auswählen. Während dieser Zeit können Anmeldeskripte ausgeführt werden oder die Benutzer können sich anmelden.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Bei Leerlauf

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Bei Leerlauf** auszuwählen.

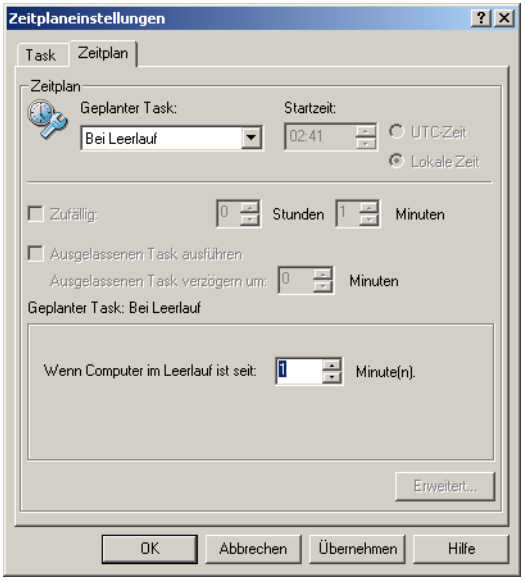


Abbildung 8-9. Registerkarte "Zeitplan" – Bei Leerlauf

2 Geben Sie unter **Task bei Leerlauf planen** die Anzahl der Minuten ein, die der Computer im Leerlauf sein soll, bevor der Task gestartet wird. Sie können einen Wert von 0 bis 999 Minuten auswählen.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Sofort ausführen

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Sofort ausführen** auszuwählen.

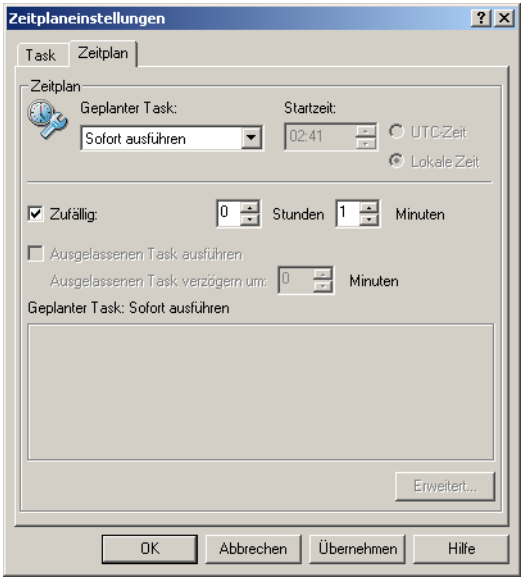


Abbildung 8-10. Registerkarte "Zeitplan" – Sofort ausführen

- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** für die maximale Zeitspanne eingeben bzw. auswählen.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben bzw. auswählen. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.

2 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Beim Einwählen ausführen

1 Gehen Sie auf der Registerkarte **Zeitplan** unter **Zeitplan** folgendermaßen vor:

- **Task planen**: Klicken Sie auf , um die Option **Beim Einwählen ausführen** auszuwählen.

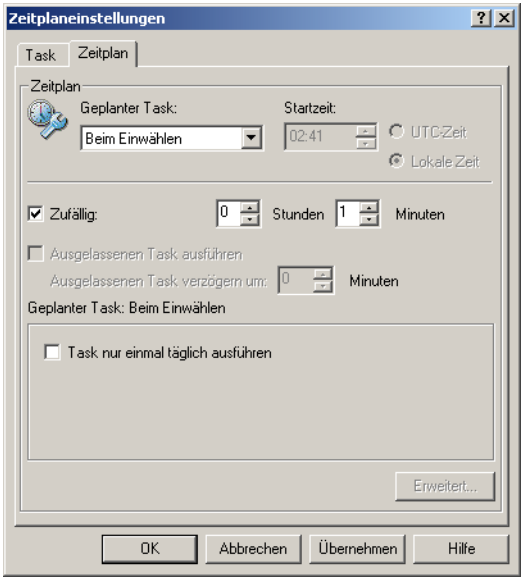


Abbildung 8-11. Registerkarte "Zeitplan" – Beim Einwählen ausführen

- **Zufällig**: Der Task wird im festgelegten Zeitraum zu einem zufällig gewählten Zeitpunkt ausgeführt. Wenn Sie diese Option wählen, müssen Sie auch die **Stunden** und **Minuten** für die maximale Zeitspanne eingeben bzw. auswählen.

  Sie können einen Zeitraum zwischen einer Minute (Minimum) und 24 Stunden (Maximum) eingeben bzw. auswählen. Wenn Sie den Task beispielsweise für 1.00 Uhr planen und ein Fenster von drei Stunden festlegen, startet der Task zu einem beliebigen Zeitpunkt zwischen 1.00 Uhr und 4.00 Uhr.

2 Geben Sie unter **Beim Einwählen ausführen** an, ob der Task einmal am Tag ausgeführt werden soll.

> **HINWEIS**
> Einen Task so zu planen, dass er **Beim Einwählen** ausgeführt wird, ist eher bei AutoUpdate-Tasks als bei Anforderungstasks sinnvoll.

3 Klicken Sie auf **OK**, um die Einstellungen zu speichern und das Dialogfeld **Zeitplaneinstellungen** zu schließen.

Befehlszeilen-Scannerprogramm A

Eine Standardinstallation der VirusScan Enterprise-Software umfasst das McAfee Security VirusScan Enterprise-Befehlszeilenprogramm. Das Programm kann über die Eingabeaufforderung von Windows aufgerufen werden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- VirusScan Enterprise -Befehlszeilenoptionen
- Befehlszeilenargumente für das Scannen auf AnforderungBefehlszeilenargumente für das Scannen auf Anforderung
- Anpassen der Installationseigenschaften

VirusScan Enterprise -Befehlszeilenoptionen

Wechseln Sie zum Starten des VirusScan Enterprise-Befehlzeilenprogramms in das Verzeichnis, in dem SCAN.EXE gespeichert ist, und geben Sie SCAN ein. Wenn Sie das Standardverzeichnis für das VirusScan Enterprise-Programm übernommen haben, befindet sich die Datei im folgenden Verzeichnis:

```
C:\Programme\Common Files\Network Associates\Engine
```

In der folgenden Tabelle finden Sie die Optionen, die Sie gemeinsam mit dem Befehl **SCAN** verwenden können. Alle aufgeführten Optionen können, sofern nicht anders angegeben, sowohl für Scans auf Anforderung als auch für Scans bei Zugriff verwendet werden.

Tabelle A-1. VirusScan-Befehlszeilenoptionen

Befehlszeilenoption	Beschreibung
/? oder /HELP	Zeigt eine Liste der Befehlszeilenoptionen von VirusScan und jeweils eine kurze Beschreibung an. Es kann u. U. zweckmäßig sein, eine Liste der Scan-Optionen zu den vom VirusScan-Programm erstellten Berichtsdateien hinzuzufügen. Geben Sie dazu an der Eingabeaufforderung Folgendes ein: scan /? /REPORT *<Dateiname>*. Daraufhin wird eine Liste aller für diesen Scan-Task verfügbaren Optionen an die Ergebnisse des Scan-Berichts angehängt.
/ADL	Scannt alle lokalen Laufwerke – auch komprimierte Laufwerke und PC-Cards, jedoch keine Disketten – zusätzlich zu allen anderen in der Befehlszeile angegebenen Laufwerken. Wenn Sie sowohl lokale Laufwerke als auch Netzwerklaufwerke scannen möchten, verwenden Sie die Befehle **/ADL** und **/ADN** zusammen in einer Befehlszeile.
/ADN	Scannt zusätzlich zu den in der Befehlszeile angegebenen Laufwerken alle Netzlaufwerke – einschließlich CD-ROMs – auf Viren. **Hinweis:** Wenn Sie sowohl lokale Laufwerke als auch Netzwerklaufwerke scannen möchten, verwenden Sie die Befehle **/ADL** und **/ADN** zusammen in einer Befehlszeile.
/ALERTPATH *<Verz>*	Legt das Verzeichnis *<Verz>* als einen Netzwerkpfad zu einem Remote-NetWare-Datenträger oder Windows NT-Verzeichnis fest. Wird durch die zentralen Warnungen überwacht. VirusScan sendet bei Entdeckung einer infizierten Datei eine ALR-Textdatei an den Server. Von diesem Verzeichnis aus verteilt oder sammelt VirusScan Enterprise über das Feature **Zentrale Warnungen** die Warnungen und Berichte entsprechend der festgelegten Konfiguration. Anforderungen: • Sie müssen für das angegebene Verzeichnis über Schreibzugriff verfügen. • Das Verzeichnis muss die von VirusScan Enterprise bereitgestellte Datei **CENTALRT.TXT** enthalten.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/ALL	Setzt die Standard-Scan-Einstellung außer Kraft und scannt alle infizierbaren Dateien – unabhängig von der Erweiterung. **Hinweise:** Bei Verwendung der Option **/ALL** erhöht sich die für den Scan-Vorgang erforderliche Zeit erheblich. Verwenden Sie diese Option nur, falls Sie einen Virus entdecken oder eine Infektion vermuten. Wenn Sie eine aktuelle Liste aller Dateityp-Erweiterungen abrufen möchten, geben Sie in der Befehlszeile /EXTLIST ein.
/ANALYZE	Weist die Software an, sowohl mit Makroheuristik als auch mit Programmheuristik zu scannen. **Hinweis: /MANALYZE** scannt nur auf Makroviren; **/PANALYZE** scannt nur auf Programmviren.
/APPEND	Zusammen mit /REPORT <*Dateiname*> verwendet, hängt diese Option den Berichtsmeldungstext an die angegebene Berichtsdatei an, anstatt die Datei zu überschreiben.
/BOOT	Scannt nur den Bootsektor und den MBR (Master Boot Record).
/CLEAN	Entfernt Viren aus allen infizierten Dateien und Systembereichen.
/CLEANDOCALL	Als Vorsichtsmaßnahme gegen Makroviren entfernt **/CLEANDOCALL** sämtliche Makros aus Microsoft Word- und Office-Dokumenten, sobald eine einzige Infektion gefunden wird. **Hinweis:** Durch die Auswahl dieser Option werden alle Makros gelöscht, einschließlich der nicht durch Viren infizierten Makros.
/CONTACTFILE <*Dateiname*>	Zeigt den Inhalt von <*Dateiname*> an, wenn ein Virus entdeckt wird. Diese Option bietet die Möglichkeit, bei Auftreten eines Virus Kontaktinformationen und Anweisungen für den Benutzer bereitzustellen. (McAfee Security empfiehlt, die Option /LOCK zusammen mit dieser Option zu verwenden.) Diese Option ist besonders in Netzwerkumgebungen nützlich, da der Text der Meldung statt auf allen lokalen Rechnern in einer zentralen Datei aufbewahrt wird. **Hinweis:** In Kontaktmeldungen können Sie alle Zeichen außer dem umgekehrten Schrägstrich (\) verwenden. Setzen Sie Meldungen, die mit einem Schrägstrich (/) oder einem Bindestrich (-) beginnen, in Anführungszeichen.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/DAM	Eine Reparaturoption, die beim Auffinden eines infizierten Makros alle Makros löscht. Wenn kein infiziertes Makro gefunden wird, erfolgt auch kein Löschvorgang. Wenn Sie den Verdacht haben, dass eine Datei infiziert ist, können Sie alle Makros aus einer Datendatei entfernen, um die Gefahr eines möglichen Virenbefalls zu minimieren. Zum präventiven Löschen aller Makros in einer Datei verwenden Sie die Option zusammen mit /FAM: scan <Dateiname> /fam /dam Bei kombinierter Verwendung dieser beiden Optionen werden alle gefundenen Makros gelöscht, unabhängig davon, ob eine Infektion gefunden wurde oder nicht.
/DEL	Löscht infizierte Dateien endgültig.
/EXCLUDE *<Dateiname>*	Scannt nicht die in *<Dateiname>* aufgeführten Dateien. Mit dieser Option können Sie bestimmte Dateien von einem Scanvorgang ausschließen. Führen Sie den vollständigen Pfad jeder auszuschließenden Datei in einer eigenen Zeile auf. Sie können die Platzhalter "*" und "?" verwenden.
/EXTLIST	Mit dieser Option können Sie eine aktuelle Liste von Dateityp-Erweiterungen aus der aktuellen DAT-Datei abrufen.
/FAM	Findet alle Makros, nicht nur Makros, bei denen eine Infektion vermutet wird. Jedes gefundene Makro wird als potenzieller Virus behandelt. Die gefundenen Makros werden nicht gelöscht, außer die Option wird zusammen mit der Option **/DAM** verwendet. Wenn Sie den Verdacht haben, dass eine Datei infiziert ist, können Sie alle Makros aus einer Datendatei entfernen, um die Gefahr eines möglichen Virenbefalls zu minimieren. Zum präventiven Löschen aller Makros in einer Datei verwenden Sie die Option zusammen mit /FAM: scan <Dateiname> /fam /dam Bei kombinierter Verwendung dieser beiden Optionen werden alle gefundenen Makros gelöscht, unabhängig davon, ob eine Infektion gefunden wurde oder nicht.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/FREQUENCY <n >	Es erfolgt kein neuer Scan-Vorgang, solange nicht **<n>** Stunden seit dem vorhergehenden vergangen sind. Verwenden Sie diese Option in Umgebungen, in denen das Risiko einer Virusinfektion niedrig ist, um unnötige Scan-Vorgänge zu vermeiden. Beachten Sie jedoch, dass der Schutz vor Vireninfektionen mit zunehmender Häufigkeit der Scan-Vorgänge steigt.
/HELP oder /?	Zeigt eine Liste der Scan-Optionen und jeweils eine kurze Beschreibung an. Es kann u. U. zweckmäßig sein, eine Liste der Scan-Optionen zu den vom VirusScan-Programm erstellten Berichtsdateien hinzuzufügen. Geben Sie dazu an der Eingabeaufforderung Folgendes ein: scan /? /REPORT <Dateiname>. Daraufhin wird eine Liste aller für diesen Scan-Task verfügbaren Optionen an die Ergebnisse des Scan-Berichts angehängt.
/LOAD <*Dateiname*>	Lädt Scan-Optionen aus der angegebenen Datei. Verwenden Sie diese Option, um einen bereits konfigurierten Scan-Vorgang durchzuführen. Hierzu werden benutzerdefinierte Einstellungen geladen, die in einer Datei im ASCII-Format gespeichert wurden.
/MANALYZE	Aktiviert die heuristische Scan-Funktion bei der Suche nach Makroviren. **Hinweis: /PANALYZE** scannt nur auf Programmviren; **/ANALYZE** scannt sowohl auf Programm- als auch auf Makroviren.
/MANY	Scannt mehrere Disketten nacheinander in einem Vorgang. Sie werden vom Programm jeweils zum Einlegen einer neuen Diskette aufgefordert. Überprüfen Sie mit dieser Option mehrere Disketten in kurzer Zeit. Sie können die Option **/MANY** nicht verwenden, wenn Sie die VirusScan-Software von einer Bootdiskette ausführen und Ihnen nur ein Diskettenlaufwerk zur Verfügung steht.
/MOVE <Verz>	Verschiebt alle während eines Scan-Vorgangs gefundenen infizierten Dateien in das angegebene Verzeichnis, wobei Laufwerksbuchstabe und Verzeichnisstruktur erhalten bleiben. **Hinweis:** Diese Option bleibt ohne Wirkung, wenn der MBR (Master Boot Record) oder der Bootsektor infiziert sind, da es sich bei diesen nicht um Dateien handelt.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/NOBEEP	Deaktiviert den Signalton, der beim Auffinden eines Virus durch den Scanner ertönt.
/NOBREAK	Deaktiviert während des Scannens die Tasten STRG+C und STRG+UNTERBR. Benutzer können bei der Verwendung von /NOBREAK den laufenden Scan-Vorgang nicht anhalten.
/NOCOMP	Überspringt die Überprüfung komprimierter ausführbarer Dateien, die mit den Dateikomprimierungsprogrammen LZ.EXE oder PkLite erstellt wurden. Wenn kein vollständiger Scan nötig ist, kann auf diese Weise die für den Scan-Vorgang benötigte Zeit verringert werden. Andernfalls sucht VirusScan in der Standardeinstellung in ausführbaren oder sich selbst dekomprimierenden Dateien nach Viren, indem jede Datei im Speicher dekomprimiert und auf Virussignaturen überprüft wird.
/NODDA	Verhindert den direkten Datenträgerzugriff. Die Scanner können somit nicht auf den Boot-Datensatz zugreifen. Diese Funktion wurde hinzugefügt, damit die Scanner unter Windows NT ausgeführt werden können. Möglicherweise müssen Sie diese Option bei einigen Laufwerken verwenden, die über Gerätetreiber angesprochen werden. Wenn Sie **/NODDA** mit den Optionen **/ADN** oder **/ADL** verwenden, können beim Zugriff auf leere CD-ROM-Laufwerke bzw. leere Zip-Laufwerke Fehler auftreten. Geben Sie in diesem Fall bei der Fehlermeldung **F** (für Fehlschlag) ein, um den Scan-Vorgang fortzusetzen.
/NOXMS	Verwendet keinen erweiterten Speicher (XMS).
/PANALYZE	Aktiviert die heuristische Scan-Funktion bei der Suche nach Programmviren. **Hinweis: /MANALYZE** scannt nur auf Makroviren; **/ANALYZE** scannt sowohl auf Programm- als auch auf Makroviren.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/PAUSE	Aktiviert die Bildschirmpause. Es wird die Aufforderung "Drücken Sie eine Taste, um fortzufahren" angezeigt, wenn das Programm einen Bildschirm mit Meldungen gefüllt hat. Anderenfalls wird der Bildschirm fortlaufend mit Meldungen gefüllt und durchgeblättert. Dies ermöglicht es, das Programm für PCs zu verwenden, die mehrere Laufwerke haben oder ernsthaft infiziert sind, ohne dass Sie eine Eingabe vornehmen müssen. McAfee Security empfiehlt, die Option /PAUSE nicht zusammen mit den Berichtsoptionen /REPORT, /RPTALL, /RPTCOR und /RPTERR) zu verwenden.
/REPORT *<Dateiname>*	Erstellt einen Bericht der infizierten Dateien und Systemfehler und speichert die Daten unter *<Dateiname>* im ASCII-Textdateiformat. Wenn *<Dateiname>* bereits vorhanden ist, wird sie von /REPORT überschrieben. Um das Überschreiben zu verhindern, verwenden Sie die Option **/APPEND** zusammen mit **/REPORT**. Die Software fügt dann Berichtsinformationen am Ende der Datei an, statt die Datei zu überschreiben. Sie können auch die Optionen **/RPTALL**, **/RPTCOR** und **/RPTERR** verwenden, um dem Bericht Angaben über gescannte, beschädigte und geänderte Dateien sowie Systemfehler hinzuzufügen. Es kann u. U. zweckmäßig sein, eine Liste der Scan-Optionen zu den vom VirusScan-Programm erstellten Berichtsdateien hinzuzufügen. Geben Sie dazu an der Eingabeaufforderung Folgendes ein: /? /report *<Dateiname>*. Daraufhin wird eine Liste aller für diesen Scan-Task verfügbaren Optionen an die Ergebnisse des Scan-Berichts angehängt. Sie können auch das Ziellaufwerk und -verzeichnis angeben (beispielsweise **D:\VSREPRT\ALL.TXT**). Wenn das Ziel jedoch ein Netzlaufwerk ist, benötigen Sie die Berechtigung zum Erstellen und Löschen von Dateien für dieses Laufwerk. McAfee Security empfiehlt, dass Sie /PAUSE nicht mit anderen Berichtsoptionen zusammen verwenden.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/RPTALL	Fügt die Namen aller gescannten Dateien in die Datei **/REPORT** ein. Sie können **/RPTCOR** und **/RPTERR** in derselben Befehlszeile verwenden. McAfee Security empfiehlt, dass Sie /PAUSE nicht mit anderen Berichtsoptionen zusammen verwenden.
/RPTCOR	Fügt beschädigte Dateien in die Datei **/REPORT** ein. In Verbindung mit **/REPORT** fügt diese Option der Berichtsdatei die Namen von beschädigten Dateien hinzu. Von VirusScan gefundene beschädigte Dateien wurden u. U. von Viren beschädigt. Sie können **/RPTCOR** und **/RPTERR** in derselben Befehlszeile verwenden. Einige Dateien, für deren ordnungsgemäße Ausführung eine Overlaydatei oder eine andere ausführbare Datei erforderlich ist (also Dateien, die sich nicht selbst ausführen), werden möglicherweise falsch gelesen. McAfee Security empfiehlt, dass Sie /PAUSE nicht mit anderen Berichtsoptionen zusammen verwenden.
/RPTERR	Fügt Fehler in die Datei **/REPORT** ein. In Verbindung mit **/REPORT** fügt diese Option der Berichtsdatei eine Liste von Systemfehlern hinzu. **/LOCK** eignet sich für sehr anfällige Netzwerkumgebungen, wie zum Beispiel frei zugängliche Computerräume. Sie können **/RPTERR** und **/RPTCOR** in derselben Befehlszeile verwenden. Bei Systemfehlern kann es sich um Probleme beim Lesen oder Schreiben auf einer Diskette oder Festplatte, Dateisystem- oder Netzwerkprobleme, Probleme beim Erzeugen von Berichten sowie andere systembezogene Probleme handeln. McAfee Security empfiehlt, dass Sie /PAUSE nicht mit anderen Berichtsoptionen zusammen verwenden.

Tabelle A-1. VirusScan-Befehlszeilenoptionen (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
/SUB	Scannt die Unterverzeichnisse eines Verzeichnisses. In der Standardeinstellung untersuchen die VirusScan-Scanner beim Auswählen eines Verzeichnisses anstelle eines Laufwerks für einen Scanvorgang nur die enthaltenen Dateien, nicht jedoch die Unterverzeichnisse. Verwenden Sie die Option **/SUB**, um alle Unterverzeichnisse der von Ihnen angegebenen Verzeichnisse zu scannen. Beim Scannen eines ganzen Laufwerks ist die Angabe von **/SUB** nicht erforderlich.
/UNZIP	Scannt komprimierte Dateien.
/VIRLIST	Zeigt den Namen jedes von der VirusScan-Software entdeckten Virus an. Die Datei ist mehr als 250 Seiten lang. Eine Datei dieser Größe kann im MS-DOS-Editor nicht geöffnet werden. McAfee Security empfiehlt daher die Verwendung des Windows-Editors oder eines anderen Texteditors zum Öffnen der Virusliste.

Befehlszeilenargumente für das Scannen auf Anforderung

Der Anforderungsscanner von VirusScan Enterprise kann über das Eingabeaufforderungsfenster von Windows oder über das Dialogfeld **Ausführen** des Menüs **Start** ausgeführt werden. Wechseln Sie zum Programmaufruf in das Verzeichnis, in dem SCAN32.EXE gespeichert ist, und geben Sie SCAN32 ein. Wenn Sie das Standardverzeichnis für das VirusScan Enterprise-Programm übernommen haben, befindet sich die Datei im folgenden Verzeichnis:

```
C:\Programme\Network Associates\VirusScan
```

In der folgenden Tabelle finden Sie die Optionen, die Sie mit dem Befehl SCAN32 verwenden können.

Tabelle A-2. Befehlszeilenargumente für das Scannen auf Anforderung

Befehlszeilenoption	Beschreibung
SPLASH	Zeigt das VirusScan-Begrüßungsdialogfeld beim Öffnen des Anforderungsscanners an.
NOSPLASH	Unterdrückt die Anzeige des VirusScan-Begrüßungsdialogfeldes beim Öffnen des Anforderungsscanners.
AUTOEXIT	Beendet den Anforderungsscanner nach Abschluss eines ohne Interaktion mit dem Benutzer ausgeführten Scan-Vorgangs.
NOAUTOEXIT	Beendet den Anforderungsscanner nach Abschluss eines ohne Interaktion mit dem Benutzer ausgeführten Scan-Vorgangs nicht.
ALWAYSEXIT	Erzwingt die Beendigung des Anforderungsscanners, auch wenn der Scan mit Fehlern abgeschlossen wurde.
NOALWAYSEXIT	Erzwingt die Beendigung nicht.
UINONE	Startet den Scanner, ohne das Konfigurationsdialogfeld zu öffnen. Dieses Argument benötigt zusätzliche Parameter zur Festlegung des Scan-Ziels.
SUB	Unterordner werden beim Scannen des Zielordners einbezogen.
NOSUB	Unterordner werden beim Scannen des Zielordners nicht einbezogen.
ALL	Scannt alle Dateien im Zielordner
NOALL	Scannt nur jene Dateien im Zielordner, deren Dateinamenerweiterungen in der Liste der festgelegten Dateitypen gefunden wurden.

Tabelle A-2. Befehlszeilenargumente für das Scannen auf Anforderung (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
COMP	Scannt Archivdateien, z. B. Dateien mit den Erweiterungen .ZIP, .CAB, .LZH und .UUE.
NOCOMP	Archivdateien vom Scan-Vorgang ausschließen.
CONTINUE	Scan-Vorgang bei Entdeckung eines Virus fortsetzen.
PROMPT	Bei Entdeckung eines Virus Benutzereingabe anfordern.
NOPROMPT	Bei Entdeckung eines Virus keine Benutzereingabe anfordern.
CLEAN	Bei Entdeckung eines Virus die infizierte Zieldatei säubern.
DELETE	Bei Entdeckung eines Virus die infizierte Datei löschen.
MOVE	Bei Entdeckung eines Virus die infizierte Datei in einen zuvor festgelegten Quarantäneordner verschieben.
BEEP	Gibt nach Abschluss eines Scanvorgangs einen Warnton aus, wenn ein infiziertes Element gefunden wurde.
NOBEEP	Unterdrückt den Warnton nach Abschluss eines Scanvorgangs, auch wenn ein infiziertes Element gefunden wurde.
RPTSIZE	Legt die Größe der Protokolldatei für Warnungen in KB fest.
BOOT	Scannt den Boot-Sektor, bevor der aktuelle Scan-Task ausgeführt wird.
NOBOOT	Schließt den Boot-Sektor vom Scan-Vorgang aus.
EXT	Von Ihnen als Parameter an dieses Argument angehängte Dateierweiterungen ersetzen die Erweiterungen auf der Liste der ausgewählten, beim Scannen zu berücksichtigenden Dateitypen.
DEFEXT	Von Ihnen als Parameter an dieses Argument angehängte Dateierweiterungen werden der Liste der ausgewählten, beim Scannen zu berücksichtigenden Dateitypen hinzugefügt.
TASK	Startet den Task für den Anforderungsscanner, wie in der VirusScan Enterprise-Konsole festgelegt. Erfordert zusätzlichen Parameter, der die entsprechende Task-ID angibt. Diese ist in der Registrierung gespeichert unter: HKEY_LOCAL_MACHINE;SOFTWARE; NETWORK ASSOCIATES;TVD; VirusScan EnterpriseNT;CurrentVersion;Tasks.

Tabelle A-2. Befehlszeilenargumente für das Scannen auf Anforderung (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
SERVER	Mit diesem Argument können Sie angeben, auf welchem Computer ein Scan-Task gestartet oder gestoppt werden soll.
CANCEL	Wenn ein Task fehlschlägt, die Konsole ihn jedoch weiterhin als aktiv anzeigt, können Sie mit diesem Argument die Registrierung dahingehend anpassen, dass der Task nicht länger als aktiv angezeigt wird.
LOG	Protokolliert Berichte zu Infektionen in einer zuvor festgelegten Protokolldatei.
NOLOG	Berichte zu Infektionen werden nicht protokolliert.
LOGALL	Protokolliert alle Reaktionen auf erkannte Viren als Ereignisse. Dazu gehören Eingabeaufforderungen, Säubern, Löschen und Verschieben.
LOGDETECT	Protokolliert das Erkennen eines Virus als Ereignis.
NOLOGDETECT	Protokolliert das Erkennen eines Virus nicht als Ereignis.
LOGCLEAN	Protokolliert Erfolg oder Fehlschlagen einer Virussäuberungsaktivität als Ereignis.
NOLOGCLEAN	Protokolliert Erfolg oder Fehlschlagen einer Virussäuberungsaktivität nicht als Ereignis.
LOGDELETE	Protokolliert das Löschen einer infizierten Datei als Ereignis.
NOLOGDELETE	Protokolliert das Löschen einer infizierten Datei nicht als Ereignis.
LOGMOVE	Protokolliert das Verschieben einer infizierten Datei in einen Quarantäneordner als Ereignis.
NOLOGMOVE	Protokolliert das Verschieben einer infizierten Datei nicht als Ereignis.
LOGSETTINGS	Protokolliert die Konfigurationseinstellungen eines Scan-Tasks.
NOLOGSETTINGS	Die Konfigurationseinstellungen eines Scan-Tasks werden nicht protokolliert.
LOGSUMMARY	Protokolliert eine Übersicht der Scan-Task-Ergebnisse.
NOLOGSUMMARY	Eine Übersicht der Scan-Task-Ergebnisse wird nicht protokolliert.
LOGDATETIME	Protokolliert das Datum, die Startzeit und die Endzeit von Scan-Aktivitäten.
NOLOGDATETIME	Datum oder Zeit von Scan-Aktivitäten werden nicht protokolliert.

Tabelle A-2. Befehlszeilenargumente für das Scannen auf Anforderung (*Fortsetzung*)

Befehlszeilenoption	Beschreibung
LOGUSER	Protokolliert die Identitätsdaten zu dem Benutzer, der einen Scan-Task ausführt.
NOLOGUSER	Benutzerdaten werden nicht protokolliert.
PRIORITY	Legt die Priorität des Scan-Tasks in Relation zu anderen CPU-Prozessen fest. Erfordert einen zusätzlichen numerischen Parameter. Der Wert 1 ordnet allen anderen CPU-Prozessen eine höhere Priorität zu. Der Wert 5 ordnet der Scan-Task die höchste Priorität zu.

Anpassen der Installationseigenschaften

Bei der Installation über die Befehlszeile können Sie den Installationsvorgang mithilfe dieser Eigenschaften anpassen.

Tabelle A-3. Angepasste Installationseigenschaften

Befehlszeileneigenschaft	Funktion
ALERTMANAGERSOURCEDIR	Stellt den Standardquellpfad des Warnungs-Managers ein. Der Standardpfad ist \AMG. Sie können diese Einstellung auch in der Datei SETUP.INI vornehmen.
CMASOURCEDIR	Stellt den Quellpfad für die Datei SITELIST.XML ein. Der Standardpfad ist das aktuelle Verzeichnis, aus dem SETUP.EXE ausgeführt wird.
ENABLEONACCESSSCANNER	False = Ein False-Wert kann nicht eingestellt werden. True = Aktiviert den Zugriffsscanner nach Abschluss der Installation. Dies ist die Standardeinstellung. **Hinweis:** Wenn Sie den Zugriffsscanner nicht aktivieren möchten, setzen Sie die Eigenschaft auf "". Das bedeutet: ENABLEONACCESSSCANNER="", eine leere Zeichenfolge.

Tabelle A-3. Angepasste Installationseigenschaften (*Fortsetzung*)

Befehlszeileneigenschaft	Funktion
EXTRADATSOURCEDIR	Stellt den Quellpfad für die Datei EXTRA.DAT ein. Während der Installation wird die Datei EXTRA.DAT an den Speicherort kopiert, an dem sich die Moduldateien befinden.
FORCEAMSINSTALL	True = Warnungs-Manager installieren, wenn vorhanden.
INSTALLDIR	Stellt das Standardinstallationsverzeichnis ein.
INSTALLCHECKPOINT	False = Check Point SCV-Integration nicht installieren. True = Check Point SCV-Integration installieren.
LOCKDOWNVIURUSSCANSHORTCUTS	False = Ein False-Wert kann nicht eingestellt werden. True = Zeigt keine Verknüpfungen im Startmenü an. **Hinweis:** Um die Installation der Verknüpfungen zu ermöglichen, setzen Sie die Eigenschaft auf "". Das bedeutet: LOCKDOWNVIURUSSCANSHORTCUTS="", eine leere Zeichenfolge. Dies ist die Standardeinstellung.
PRESERVESETTINGS	Beibehalten der Einstellungen beim Upgrade von NetShield 4.5 oder VirusScan 4.5.1. False = Ein False-Wert kann nicht eingestellt werden. True = Einstellungen beibehalten. Dies ist die Standardeinstellung. **Hinweis:** Wenn Sie die Einstellungen nicht beibehalten möchten, setzen Sie die Eigenschaft auf "". Das bedeutet: PRESERVESETTINGS="", eine leere Zeichenfolge.

Tabelle A-3. Angepasste Installationseigenschaften (*Fortsetzung*)

Befehlszeileneigenschaft	Funktion
RUNAUTOUPDATE	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation AutoUpdate aus. Dies ist die Standardeinstellung. **Hinweis:** Wenn AutoUpdate nach Abschluss der Installation nicht ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNAUTOUPDATE="", eine leere Zeichenfolge.
RUNONDEMANDSCAN	False = Ein False-Wert kann nicht eingestellt werden. True = Scannt alle lokalen Laufwerke nach Abschluss der Installation. Dies ist die Standardeinstellung. **Hinweis:** Wenn der Anforderungsscanner nach Abschluss der Installation nicht ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: PRUNONDEMANDSCAN="", eine leere Zeichenfolge.
RUNAUTOUPDATESILENTLY	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation eine automatische Aktualisierung aus. **Hinweis:** Wenn nach Abschluss der Installation keine automatische Aktualisierung ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNAUTOUPDATESILENTLY="", eine leere Zeichenfolge.
RUNONDEMANDSCANSILENTLY	False = Ein False-Wert kann nicht eingestellt werden. True = Führt nach Abschluss der Installation einen automatischen Anforderungsscan aus. **Hinweis:** Wenn nach Abschluss der Installation kein automatischer Anforderungsscan ausgeführt werden soll, setzen Sie die Eigenschaft auf "". Das bedeutet: RUNONDEMANDSCANSILENTLY="", eine leere Zeichenfolge.

Tabelle A-3. Angepasste Installationseigenschaften (*Fortsetzung*)

Befehlszeileneigenschaft	Funktion
SUPPRESSAMSINSTALL	True = Unterdrückt die Installation von Alert Manager.
VIRUSSCANICONLOCKDOWN	Sperrt das Produkt auf zwei verschiedenen Ebenen. NORMAL = Zeigt alle Menüelemente im VirusScan-Kontextmenü in der Statusleiste an. Dies ist die Standardeinstellung. MINIMAL = Zeigt nur die Menübefehle **Scannen bei Zugriff aktivieren** und **Info zu VirusScan Enterprise** im VirusScan-Kontextmenü in der Statusleiste an. NOICON = Zeigt das VirusScan-Kontextmenü in der Statusleiste nicht an.

Sichere Registrierung B

Das VirusScan Enterprise-Programm ist kompatibel mit dem Windows-Feature für die Sicherung der Registrierung. Das Programm hält sich beim Schreiben von Registrierungseinträgen an die durch die Sicherheitseinstellungen für den Benutzer vorgegebenen Grenzwerte. Jedes Programmfeature, für das der Benutzer nicht über die entsprechende Berechtigung verfügt, ist deaktiviert. Es kann somit vom Benutzer weder ausgewählt werden, noch reagiert es auf Eingaben. In früheren Versionen des Produkts wurden manchmal Fehler ausgelöst, wenn das VirusScan Enterprise-Programm versucht hat, einen Registrierungseintrag für eine Funktion zu schreiben, für die der Benutzer keine Berechtigung hatte.

Dieses Thema ist in diesem Abschnitt enthalten:

- *Registrierungsschlüssel, für die Schreibzugriff erforderlich ist*

Registrierungsschlüssel, für die Schreibzugriff erforderlich ist

Im Folgenden finden Sie eine Liste von Registrierungsschlüsseln, zu denen VirusScan Enterprise und die Alert Manager-Komponente Schreibzugriff benötigen. Die Tabelle zeigt auch die Ergebnisse, die eintreten, wenn der Benutzer nicht über die entsprechende Schreiberlaubnis auf diese Schlüssel verfügt.

Alle in dieser Tabelle aufgeführten Registrierungsschlüssel sind Unterschlüssel von:

```
hkey_local_machine\software\network associates\tvd.
```

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
On Access Scanner	McShield-Dienst von Network Associates	Ein Windows-Dienst, der nur unter dem lokalen Systemkonto ausgeführt werden kann. Dieser Dienst führt bei jeder Verwendung einer Datei einen Scan aus.	Shared Components On Access Scanner	Normalerweise keine Auswirkung, da der Dienst unter einem Systemkonto ausgeführt wird. Wenn der Dienst jedoch keinen Schreibzugriff für diesen Schlüssel besitzt, funktioniert der Zugriffsscanner nicht.
On Access Scanner	ShCfg32.exe	Ein Programm, das die Zugriffskonfigurations-oberfläche ausführt.	Shared Components On Access Scanner McShield Configuration	Der Benutzer kann die Eigenschaftenseiten für den Zugriffsscanner anzeigen, die Konfiguration jedoch nicht ändern.

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
On Access Scanner	ShStat.exe	Ein Programm, das Statistiken zu den Aktivitäten des Zugriffsscanners sammelt. Das Programm ist auch für das VirusScan Enterprise-Symbol in der Taskleiste zuständig. Durch einen Klick mit der rechten Maustaste auf das Symbol kann der Benutzer die Scan-Statistiken anzeigen, das Programm de-/aktivieren sowie verschiedene Programmkomponenten öffnen.	Shared Components On Access Scanner McShield Configuration	Der Benutzer kann den Zugriffsscanner nicht über das Symbol in der Taskleiste (de-)aktivieren
Anforderungs scanner	ScnCfg32	Ein Programm, das die Anforderungs-Konfigurationsoberfläche ausführt. Auf die Oberfläche wird über die VirusScan Enterprise-Konsole zugegriffen.	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion DefaultTask VirusScan Enterprise CurrentVersion Tasks	Wenn der Schreibzugriff für einen dieser Schlüssel fehlschlägt, kann der Benutzer die Eigenschaftenseiten für den Anforderungsscanner zwar anzeigen, die Konfiguration jedoch nicht ändern.

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
Anforderungs scanner	ScnStat.exe	Ein Programm, das Statistiken zu den Aktivitäten des Anforderungsscanners sammelt.	VirusScan Enterprise CurrentVersion Tasks VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion Tasks	Keine Auswirkung.
Anforderungs scanner	Scan32.exe	Ein Programm, das die Anforderungsscan-Aktivitäten für die in der VirusScan Enterprise-Konsole festgelegten Ziele durchführt.	VirusScan Enterprise CurrentVersion VirusScan Enterprise CurrentVersion\ Tasks **Hinweis:** Außerdem sind Leseberechtigungen nötig für: • Shared Components • VirusScan Engine • 4.0.xx	Wenn Scan32 nicht über einen Schlüssel mit Schreibrechten für seinen eigenen Task verfügt, wird es zwar ausgeführt, aktualisiert jedoch nicht die Statistik. Es werden keine Ergebnisdaten für den Scan erzeugt. Geplante Anforderungs-Tasks sind davon nicht betroffen. Diese werden von dem im folgenden Abschnitt beschriebenen Task-Manager-Dienst gesteuert.

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
Task-Manager	Network Associates-Task-Manager-Dienst	Ein Windows-Dienst, der unter dem Systemkonto oder dem Administratorkonto ausgeführt werden kann. Dieses Programm ermöglicht die Planung von Scan- und Aktualisierungsaktivitäten.	VirusScan Enterprise NT CurrentVersion VirusScan Enterprise NT CurrentVersion Warnungen VirusScan Enterprise NT CurrentVersion Tasks alle Unterschlüssel Shared Components On Access Scanner McShield Shared Components On-Access scanner McShield Configuration	Normalerweise keine Auswirkung, da der Dienst unter einem System- oder Administratorkonto ausgeführt wird. Wenn der Dienst jedoch keinen Lese-/Schreibzugriff für einen dieser Schlüssel besitzt, kann der Dienst nicht gestartet werden.

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
McUpdate	McUpdate.exe	Ein Programm, das zum Aktualisieren von DAT -Dateien sowie für Softwareupgrades verwendet wird	VirusScan Enterprise NT CurrentVersion Shared Components On Access Scanner McShield Configuration	DAT-Informationen werden nicht aktualisiert. McShield kann u. U. die DAT nicht neu laden. Statusinformationen können nicht an die VirusScan Enterprise-Konsole weitergegeben werden.
			VirusScan Enterprise NT CurrentVersion Tasks	Der Benutzer kann die Eigenschaftenseite für die Aktualisierung anzeigen, die Konfiguration jedoch nicht ändern.
			VirusScan Enterprise NT CurrentVersion Tasks Update	Der Benutzer kann die Eigenschaftenseite für das Upgrade anzeigen, die Konfiguration jedoch nicht ändern.
			VirusScan Enterprise NT CurrentVersion Tasks Upgrade	

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
VirusScan Enterprise-Konsole	McConsol.exe	Ein Programm, das die Verwaltungsoberfläche für das VirusScan Enterprise-Programm ausführt.	VirusScan Enterprise NT CurrentVersion VirusScan Enterprise NT CurrentVersion Warnungen CurrentVersion VirusScan Enterprise NT CurrentVersion Tasks Shared Components On Access Scanner McShield Configuration VirusScan Enterprise NT CurrentVersion Tasks Xxxx	Die Aktualisierung der Virusdefinitionen funktioniert nicht zuverlässig. Außerdem kann der Benutzer die aktuelle Bildschirmaktualisierungsrate zwar anzeigen, sie jedoch nicht ändern. Die bei Auswahl der Option "Warnungen" aus dem Menü "Extras" angezeigten Warnungs-Manager-Einstellungen sind deaktiviert und reagieren nicht auf Eingaben. Außerdem werden bestimmte von der VirusScan Enterprise-Konsole gesteuerte Start-/Stop-Tasks u. U. nicht generiert. Die folgenden Optionen sind deaktiviert und reagieren nicht: • Aktivieren/Deaktivieren des Zugriffsscan-Tasks. • Kopieren, Einfügen, Löschen, Umbenennen, Importieren und Exportieren von Tasks. • Scan-Steuerelement zum Stoppen.

Tabelle B-1. VirusScan Enterprise – Ergebnisse der Registrierungsschlüsselsperrung (*Fortsetzung*)

Funktion	Programm oder Windows-Dienst	Beschreibung	Für volle Funktionalität Schreibzugriff auf Registrierungs-schlüssel nötig	Ergebnis, wenn wegen Registrierungssperrung kein Schreibzugriff möglich
VirusScan Enterprise-Konsole *(fortsetzung)*	McConsol.exe *(fortsetzung)*	Ein Programm, das die Verwaltungsoberfläche für das VirusScan Enterprise-Programm ausführt *(fortsetzung)*		Gesperrte Schlüssel können nicht konfiguriert werden.
Warnungs-Manager	NAI Warnungs-Manager	Eine Komponente, die sofortige Benachrichtigungen generiert, wenn der Scanner einen Virus entdeckt hat oder wenn der Ereignisplaner auf ein Problem gestoßen ist.	Shared Components Warnungs-Manager	Der Benutzer kann die Eigenschaftenseiten für die Warnmethoden und -meldungen anzeigen, die Konfiguration jedoch nicht ändern.

Fehlerbehebung C

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in VirusScan Enterprise.

In diesem Abschnitt werden die folgenden Themen behandelt:

- Minimum Escalation Tool
- Häufig gestellte Fragen
- Aktualisieren von Fehlercodes

Minimum Escalation Tool

Das McAfee Minimum Escalation Tool (MERTool) ist ein Dienstprogramm, das Berichte und Protokolle für die Network Associates-Software auf Ihrem System erfasst. Die dadurch gewonnenen Informationen können beim Analysieren von Problemen hilfreich sein.

Weitere Informationen zum MERTool und zum Zugriff auf das Dienstprogramm erhalten Sie, wenn Sie auf die Datei *MERTool* klicken, die mit VirusScan Enterprise installiert wurde.

Diese Datei befindet sich im Installationsverzeichnis. Wenn Sie den standardmäßigen Installationspfad übernommen haben, wird die Datei im folgenden Pfad abgelegt:

```
Laufwerk:\Programme\Network Associates\VirusScan
```

Wenn Sie auf die Datei *MERTool* klicken, greift diese auf den URL für die MERTool-Website zu. Befolgen Sie die Anweisungen auf der Website.

Häufig gestellte Fragen

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Form von häufig gestellten Fragen. Die Fragen wurden in folgende Kategorien unterteilt:

- Fragen zur Installation
- Fragen zum Scannen
- Fragen zu Viren
- Allgemeine Fragen

Fragen zur Installation

Ich habe die Software mit der unbeaufsichtigten Installationsmethode installiert; es wird jedoch kein VirusScan Enterprise-Symbol in der Windows-Systemablage angezeigt.

Das Symbol wird erst nach einem System-Neustart in der Systemablage angezeigt. VirusScan Enterprise wird aber trotzdem ausgeführt, sodass Ihr Computer auch dann geschützt wird, wenn kein Symbol angezeigt wird.

Sie können dies durch Überprüfung des folgenden Registrierungsschlüssels testen:

HKEY_Local_Machine\SOFTWARE/Microsoft\Windows\CurrentVersion\Run
ShStatEXE="C:\Program Files\Network
Associates\VirusScan\SHSTAT.EXE\STANDALONE

Warum können in meinem Netzwerk nur bestimmte Benutzer eigene Einstellungen in VirusScan Enterprise konfigurieren?

Wenn der Administrator die Benutzeroberfläche so konfiguriert, dass die Tasks durch Kennwörter geschützt sind, können die Benutzer die Einstellungen nicht ändern.

Bei verschiedenen Microsoft Windows-Betriebssystemen bestehen unterschiedliche Benutzerberechtigungen. Windows NT-Benutzer verfügen über eine Schreibberechtigung für die Systemregistrierung, die Benutzer von Windows XP oder Windows 2000 nicht haben. Weitergehende Informationen zu den Berechtigungen erhalten Sie in der Microsoft Windows-Dokumentation.

Wie kann ich während einer Befehlszeileninstallation verhindern, dass Benutzer ohne Administratorrechte diese über die VirusScan-Konsole erhalten?

Damit solchen Benutzern Administratorrechte nicht unberechtigterweise zugewiesen werden, müssen Sie in einer Befehlszeileninstallation folgende Eigenschaft hinzufügen:

DONOTSTARTSHSTAT=True

Dadurch wird verhindert, dass SHSTAT.EXE nach Abschluss der Installation gestartet wird.

Fragen zum Scannen

Worin besteht beim Zugriffsscan der Unterschied zwischen dem Scannen "Beim Schreiben auf den Datenträger" und "Beim Lesen vom Datenträger"?

Scannen beim Schreiben ist ein Dateischreibvorgang. Dabei werden folgende Elemente überprüft:

- Eingehende Dateien, die auf die lokale Festplatte geschrieben werden.
- Dateien, die auf der lokalen Festplatte oder einem zugeordneten Netzlaufwerk erstellt werden (einschließlich neuer, geänderter oder zwischen Laufwerken kopierter bzw. verschobener Dateien).

Scannen beim Lesen ist ein Dateilesevorgang. Dabei werden folgende Elemente überprüft:

- Ausgehende Dateien, die von der lokalen Festplatte gelesen werden.

  HINWEIS
  Wählen Sie im Dialogfeld **Eigenschaften des Scannens bei Zugriff** die Option **Auf Netzlaufwerken**, um entfernte Netzwerkdateien hinzuzufügen.

- Alle auf der lokalen Festplatte ausgeführten Dateien.
- Alle auf der lokalen Festplatte geöffneten Dateien.
- Alle auf der lokalen Festplatte umbenannten Dateien, wenn dabei die Dateieigenschaften geändert wurden.

Welche Bedeutung haben die unterschiedlichen Aktionsoptionen beim Erkennen eines Virus mit der E-Mail-Scan-Methode auf Anforderung oder der E-Mail-Scan-Methode bei Empfang?

Eine detaillierte Beschreibung der einzelnen Aktionsoptionen finden Sie unter *Aktionseigenschaften* auf Seite 135.

Fragen zu Viren

Ich habe vermutlich einen Virus, der aber von VirusScan Enterprise nicht erkannt wird.

Sie können die neueste DAT-Datei bereits vor dem offiziellen Release herunterladen, wenn sie noch in der Testphase ist. Die jeweils gültige DAT-Datei finden Sie unter:

www.mcafeeb2b.com/naicommon/avert/avert-research-enter/virus-4d.asp

Ich kann VirusScan Enterprise nicht installieren, habe aber vermutlich einen Virus. Wie kann ich feststellen, ob mein Computer infiziert ist?

Wenn Sie VirusScan Enterprise nicht installieren können, ist die Ausführung eines Scan-Vorgangs immer über die Befehlszeile mit einer einzelnen von der Network Associates-Website heruntergeladenen Datei möglich. So führen Sie auf einem Computer ohne installierte Antivirensoftware einen Befehlszeilen-Scan aus:

1. Erstellen Sie im Stammverzeichnis von Laufwerk C einen Ordner mit dem Namen "Scan".
2. Klicken Sie mit der rechten Maustaste auf den Ordner, und wählen Sie **Eigenschaften** aus. Stellen Sie sicher, dass das Schreibschutz-Attribut aktiviert ist.
3. Rufen Sie die Seite http://nai.com/naicommon/download/dats/superdat.asp auf. Klicken Sie auf **sdatxxxx.exe für Windows-Intel**, um den Download zu starten.
4. Laden Sie diese Datei in den neuen Ordner (`C:\Scan`) herunter.
5. Wählen Sie im Menü **Start** die Option **Ausführen**, und geben Sie in das Textfeld `C:\Scan\sdatxxxx.exe /e` ein. Klicken Sie auf **OK**.
6. Öffnen Sie die DOS-Eingabeaufforderung (auch Befehlszeile genannt). Geben Sie an der Eingabeaufforderung **`C:\>`** den Befehl `cd C:\Scan` ein. Die Eingabeaufforderung sieht dann folgendermaßen aus: **`C:\Scan>`**
7. Geben Sie an der Eingabeaufforderung **`C:\Scan>`** Folgendes ein:

   ```
   scan.exe /clean /all /adl /unzip /report report.txt
   ```

   Damit werden alle lokalen Laufwerke überprüft, und in der Datei REPORT.TXT wird ein Bericht erstellt.
8. Navigieren Sie nach der Überprüfung zu dem Verzeichnis **`C:\Scan`**, und öffnen Sie die Datei REPORT.TXT.

HINWEIS
Es wird empfohlen, die Netzwerkverbindung des Systems vor dem Scannen zu trennen.

Starten Sie Windows 2000- und Windows XP-Systeme für den Scan-Vorgang nur im abgesicherten Eingabeaufforderungsmodus. Führen Sie den Scan-Vorgang über die Eingabeaufforderung auf Windows NT-Systemen im VGA-Modus aus.

Es wird empfohlen, den Befehlszeilenscanner so lange auszuführen, bis keine Viren mehr gefunden werden. Sie können die Berichtstextdatei für den zweiten, dritten und jeden weiteren Scan-Vorgang in REPORT2.TXT, REPORT3.TXT usw. umbenennen und somit vermeiden, dass die Berichtsdatei jedes Mal überschrieben wird.

WARNUNG
Unter Umständen erhalten Sie eine Fehlermeldung, weil eine Anwendung direkt auf die Festplatte des Windows NT-Systems zuzugreifen versucht. Klicken Sie zum Fortfahren auf **Ignorieren**. Anderenfalls wird der Scan-Vorgang abgebrochen.

Allgemeine Fragen

Das VirusScan Enterprise-Symbol in der Systemablage ist anscheinend deaktiviert.

Wenn auf dem VirusScan Enterprise-Symbol ein durchgestrichener roter Kreis angezeigt wird, ist das Scannen bei Zugriff deaktiviert. Die häufigsten Ursachen und die jeweiligen Lösungen werden im Folgenden aufgeführt. Wenn das Problem dennoch fortbesteht, wenden Sie sich an den Technischen Support.

- Überprüfen Sie, ob Scannen bei Zugriff aktiviert ist. Gehen Sie dazu folgendermaßen vor:
  - Klicken Sie mit der rechten Maustaste auf das VirusScan Enterprise-Symbol in der Systemablage. Wenn der Zugriffsscanner deaktiviert ist, wird im Menü **Scannen bei Zugriff aktivieren** angezeigt.
  - Wählen Sie zum Aktivieren des Zugriffsscanners die Option **Scannen bei Zugriff aktivieren**.
- Stellen Sie sicher, dass der Dienst ausgeführt wird. Gehen Sie dazu folgendermaßen vor:
  - Öffnen Sie das Applet "Dienste" in der Systemsteuerung anhand einer der folgenden Methoden:
    - Wählen Sie unter Windows NT **Start** | **Einstellungen** | **Systemsteuerung** | **Dienste**, und überprüfen Sie, ob **Network Associates McShield** den Status **Gestartet** aufweist.
    - Bei Windows 2000 oder XP wählen Sie **Start** | **Einstellungen** | **Systemsteuerung** | **Verwaltung** | **Dienste**, und überprüfen Sie, ob **Network Associates McShield** den Status **Gestartet** aufweist.
  - Wenn der Dienst nicht gestartet wurde, markieren Sie **Network Associates McShield** in der Diensteliste, und klicken Sie dann auf **Starten** oder **Fortsetzen**.

    Alternativ haben Sie die Möglichkeit **Start** | **Ausführen** auszuwählen und dann **NetStart McShield** einzugeben.

- Stellen Sie sicher, dass für den Dienst automatisches Starten eingestellt ist. Gehen Sie dazu folgendermaßen vor:
  - Öffnen Sie das Applet "Dienste" in der Systemsteuerung anhand einer der folgenden Methoden:
    - Wählen Sie unter Windows NT **Start** | **Einstellungen** | **Systemsteuerung** | **Dienste**, und überprüfen Sie, ob **Network Associates McShield** den Startyp **Automatisch** aufweist.

      Wenn der Starttyp nicht auf **Automatisch** eingestellt ist, markieren Sie in der Liste der Dienste die Option **Network Associates McShield**, klicken Sie auf **Start**, und wählen Sie dann als Starttyp die Option **Automatisch**.
    - Bei Windows 2000 oder XP wählen Sie **Start** | **Einstellungen** | **Systemsteuerung** | **Verwaltung** | **Dienste**, und überprüfen Sie, ob **Network Associates McShield** den Starttyp **Automatisch** aufweist.

      Wenn der Starttyp nicht auf **Automatisch** eingestellt ist, klicken Sie mit der rechten Maustaste in der Liste der Dienste auf **Network Associates McShield**, wählen Sie **Eigenschaften** und die Registerkarte **Allgemein**, und wählen Sie dann als Starttyp die Option **Automatisch**.

Ich erhalte eine Fehlermeldung, dass die Datei "catalog.z" nicht heruntergeladen werden kann.

Diesem Fehler können verschiedene Ursachen zugrunde liegen. Im Folgenden werden nur einige Empfehlungen zur Feststellung der Problemursache gegeben.

- **Wenn Sie die Standard-Download-Site von Network Associates für Aktualisierungen** verwenden, überprüfen Sie, ob Sie die Datei `catalog.z` über einen Webbrowser herunterladen können. Rufen Sie dazu folgenden URL auf:

  http://update.nai.com/Products/CommonUpdater/catalog.z

  Versuchen Sie, die Datei herunterzuladen.
  - Wenn Sie die Datei sehen, aber *nicht* herunterladen können (d. h., dass der Browser das Herunterladen verhindert), weist das auf ein Proxy-Problem hin, das Sie mit Ihrem Netzwerkadministrator besprechen müssen.
  - Wenn das Herunterladen der Datei *möglich* ist, müsste dies auch mit VirusScan Enterprise möglich sein. Weitere Unterstützung bei der Fehlerbehebung in VirusScan Enterprise erhalten Sie vom Technischen Support.
- **Wenn Sie eine Spiegelungs-Site für Aktualisierungen** verwenden, müssen Sie sicherstellen, dass diese Spiegelungs-Site auf die richtige Site für Updates verweist. Im Zweifelsfall sollten Sie die Einstellungen so ändern, dass Sie die Network Associates-Standardsite verwenden können.

Auf einigen Computern wird noch VirusScan 4.5x und auf anderen VirusScan Enterprise 7.0 verwendet. Können alle Computer dasselbe Repository für DAT-Dateien verwenden?

Ja, ein Computernetzwerk mit mehreren VirusScan-Versionen kann dasselbe Repository für DAT-Dateien verwenden. Vergewissern Sie sich zunächst, dass Sie die richtige Verzeichnisstruktur in der Repository-Liste für VirusScan 4.5.x verwenden. Überprüfen Sie dann, ob Sie in der Konsole von McAfee AutoUpdate Architect die Option **Ich möchte meine Site mit Legacy-Software kompatibel machen** ausgewählt wurde. Weitere Informationen finden Sie im *Produkthandbuch zu McAfee AutoUpdate Architect*.

Wo befindet sich die HTTP-Download-Site?

Die Datei CATALOG.Z, die die neuesten Aktualisierungen enthält, kann von folgender Website heruntergeladen werden:

http://update.nai.com/Products/CommonUpdater/catalog.z

Wo befindet sich die FTP-Download-Site?

Die Datei CATALOG.Z, die die neuesten Aktualisierungen enthält, kann von folgender FTP-Site heruntergeladen werden:

ftp://ftp.nai.com/CommonUpdater/catalog.z

Wenn bei Verwendung der Option "Benutzereingabe anfordern" ein Virus erkannt wird, welche Aktion sollte ich auswählen (Säubern, Löschen, Verschieben)?

Generell wird empfohlen, die Aktion **Säubern** zu wählen, wenn Sie nicht genau wissen, wie Sie mit der infizierten Datei umgehen sollten. Standardmäßig wird in VirusScan Enterprise eine Datei **gesäubert** und anschließend **verschoben**.

Das Verschieben oder Löschen einer Datei ist fehlgeschlagen.

Das ist möglich, wenn eine Datei von einem anderen Programm gesperrt ist, oder Sie nicht die entsprechenden Berechtigungen zum Verschieben oder Löschen der Datei haben. Als Lösung des Problems sollten Sie den Speicherort der Datei dem VirusScan Enterprise-Protokoll entnehmen und die Datei manuell in Windows Explorer verschieben bzw. löschen.

Aktualisieren von Fehlercodes

Wenn AutoUpdate fehlschlägt, überprüfen Sie das Aktualisierungsprotokoll. Weitere Informationen zum Anzeigen der Protokolldatei finden Sie unter *Anzeigen des Aktivitätsprotokolls* auf Seite 210. Im Folgenden finden Sie häufige Fehlercodes, auf die Sie stoßen könnten:

- **-215: Standort-Status konnte nicht abgerufen werden** – Die Software kann nicht feststellen, ob das Repository verfügbar ist. Versuchen Sie, die Datei PKGCATALOG.Z mithilfe des Netzwerkprotokolls manuell herunterzuladen. Wenn dieses nicht möglich ist, überprüfen Sie den Pfad und die Login-Informationen.
- **-302: Die Framework-Schnittstelle des Agenten konnte nicht abgerufen werden** – Die Planer-Schnittstelle ist nicht verfügbar. Halten Sie den Framework-Dienst an und starten Sie ihn neu.
- **-409: Master-Standort nicht gefunden** – Das Master-Repository für die Aktualisierung ist nicht verfügbar, wird bereits verwendet, oder es kann nicht darauf zugegriffen werden. Versuchen Sie, die Datei PKGCATALOG.Z mithilfe des Netzwerkprotokolls manuell herunterzuladen. Wenn diese nicht möglich ist, überprüfen Sie den Pfad und die Login-Informationen.
- **-414: Überprüfen Sie, ob Domäne, Benutzername und Kennwort korrekt eingegeben wurden. Vergewissern Sie sich, dass das Benutzerkonto Berechtigungen für den Speicherort hat, an dem sich das Repository befindet** – Bei der Erstellung des Repository stellten sich die eingegebenen Anmeldedaten bei Auswahl von **Prüfen** als ungültig heraus. Korrigieren Sie die Anmeldedaten entweder sofort oder nachdem das Repository erstellt wurde. Klicken Sie erneut auf **Prüfen**. Wiederholen Sie diesen Vorgang, bis alle Anmeldedaten überprüft wurden.
- **-503: Produktpaket nicht gefunden** – Es sind keine Aktualisierungsdateien im Repository vorhanden, oder sie sind beschädigt. Vergewissern Sie sich, dass die Aktualisierungsdateien im Repository enthalten sind. Wenn diese Dateien vorliegen, erstellen Sie eine Replizierung oder einen Pull-Task, um die aktuelle Task-Einstellung zu überschreiben. Wenn die Dateien nicht vorliegen, bringen Sie sie in das Repository, und versuchen Sie dann erneut, die Aktualisierung vorzunehmen.
- **-530: Standortkatalog nicht gefunden** – Sie haben einen Pull-Task von einem Repository aus vorgenommen, das keine Katalogdatei aufweist oder dessen Katalogdatei beschädigt ist. Um dieses Problem zu beheben, müssen Sie sicherstellen, dass das Ausgangs-Repository ein gültiges Katalogverzeichnis enthält.
- **-531: Paketkatalog nicht gefunden** – Die Datei PKGCATALOG.Z wurde nicht im Repository gefunden. Versuchen Sie, die Datei mithilfe des Netzwerkprotokolls herunterzuladen. Wenn sie nicht heruntergeladen werden kann, führen Sie eine Replizierung oder einen Pull-Task durch (je nach Repository-Typ).

- **-601: Datei konnte nicht heruntergeladen werden** – Das Repository ist nicht verfügbar. Versuchen Sie, die Datei mithilfe des Netzwerkprotokolls herunterzuladen. Wenn sie nicht heruntergeladen werden kann, überprüfen Sie den Pfad und die Benutzerberechtigungen. Wenn die Datei heruntergeladen werden konnte, halten Sie den Dienst an, und starten Sie ihn erneut.
- **-602: Datei konnte nicht hochgeladen werden** – Sie haben einen Pull-Task durchgeführt, die Anmeldeinformationen oder die Einstellungen für das Master-Repository sind jedoch ungültig (oder der Speicherort ist nicht verfügbar). Überprüfen Sie die Anmeldeinformationen und den Speicherort.
- **-804: Standort-Status nicht gefunden** – Sie haben einen Replizierungs-Task durchgeführt, doch das Master-Repository ist nicht verfügbar (oder die Anmeldeinformationen sind ungültig). Vergewissern Sie sich, dass das Master-Repository aktiv und zugänglich ist, und dass die Anmeldeinformationen gültig sind.
- **-1113: Replizierung wurde teilweise durchgeführt** – Zum Zeitpunkt der Replizierung waren möglicherweise ein oder mehrere Repositories nicht verfügbar. Daher sind nicht alle Repositories auf dem neuesten Stand. Vergewissern Sie sich, dass der Zugriff auf alle Repositories möglich ist und dass keine Dateien als *schreibgeschützt* gekennzeichnet sind, und führen Sie den Task anschließend erneut aus.

Glossar

.MSI-Datei
Ein Microsoft Windows Installer-Paket, das Installations- und Konfigurationsanweisungen für die bereitzustellende Software enthält.

.NAP-Datei
Network Associates-Paketdatei. Diese Dateierweiterung wird zur Bezeichnung von McAfee-Software-Programmdateien verwendet, die im Software-Repository installiert sind, damit sie von ePolicy Orchestrator verwaltet werden können.

Agent
Siehe *ePolicy Orchestrator-Agent*.

Agentenreaktivierung
Ein geplanter Task oder Anforderungsbefehl, der Agenten auffordert, bei Bedarf Kontakt mit dem ePolicy Orchestrator-Server aufzunehmen, anstatt auf den nächsten ASCI-Befehl zu warten.

Siehe auch SuperAgent-Reaktivierung.

Agentenrichtlinien
Einstellungen, die das Verhalten des Agenten beeinflussen.

Agent-Host
Siehe Client-Computer.

Agent-Monitor
Ein Dialogfeld, um Agenten aufzufordern, Eigenschaften oder Ereignisse an den ePolicy Orchestrator-Server zu senden, Richtlinien und Tasks lokal durchzusetzen, den ePolicy Orchestrator-Server auf neue oder aktualisierte Richtlinien und Tasks zu prüfen und sie dann sofort bei Erhalt umzusetzen.

Agent-zu-Server-Kommunikation
Ein Kommunikationsverfahren, bei dem der Agent in vordefinierten Intervallen Kontakt mit dem Server aufnimmt, um zu überprüfen, ob neue Richtlinien oder Tasks vorliegen, die der Agent durchsetzen oder ausführen muss.

Agent-zu-Server-Kommunikationsintervall (ASCI)
Bestimmt, wie oft der Agent und der ePolicy Orchestrator-Server Informationen austauschen.

Aktualisieren
Die Installation von Aktualisierungen für bestehende Produkte oder die Aktualisierung auf neue Produktversionen.

Aktualisierungspaket
Paketdateien von Network Associates, die Aktualisierungen für ein Produkt bieten. Alle Pakete werden als Produktaktualisierungen betrachtet, mit Ausnahme der binären Produkt-(Setup-)Dateien.

Alternativ-Repository
Das Repository, aus dem Client-Computer Aktualisierungen abrufen, wenn keines der Repositories in ihrer Repository-Liste (SITELIST.XML) verfügbar ist. Es kann nur ein einziges Alternativ-Repository definiert werden.

Antivirenrichtlinie
Siehe Richtlinie.

Archiv
Eine komprimierte Datei, die extrahiert werden muss, bevor auf die darin enthaltenen Dateien zugegriffen werden kann.

Ausbringung
Senden von Produkten (und des Agents) an Gruppen, Computer und Benutzer und Installation.

Ausgehendes Scannen
Vergleiche Eingehendes Scannen.

Automatische Installation
Eine Installationsmethode, die ein Software-Paket auf einem Computer automatisch installiert, ohne dass der Benutzer aktiv werden muss.

AutoUpdate
Das Programm für die automatische Aktualisierung bei McAfee Security-Antivirus-Produkten. Es installiert Aktualisierungen zu bestehenden Produkten oder Upgrades auf neue Versionen der Produkte automatisch.

AVERT
Anti-Virus Emergency Response Team, ein Bereich von Network Associates, Inc., ist ein Antivirus-Forschungszentrum, das die Öffentlichkeit und Kunden von Network Associates durch die Erforschung der neuesten Bedrohungen und der Aufdeckung von künftigen Bedrohungen unterstützt. Der Bereich besteht aus drei integrierten Teams, die Antiviren-Services und -Support, Virenanalyse und fortschrittliche Virenforschung bieten.

Benutzerkonten
Zu den ePolicy Orchestrator-Benutzerkonten gehören der globale Administrator, der globale Prüfer, der Standortadministrator und der Standortprüfer. Benutzerkonten auf Administratorebene verfügen über Lese-, Schreib- und Löschberechtigungen; Benutzerkonten auf Prüferebene verfügen nur über Leseberechtigungen.

Siehe auch Globaler Administrator, Globaler Prüfer, Standortadministrator und Standortprüfer.

Bereich
Ein Unterabschnitt der Konsole.

Siehe Detailbereich und Konsolenstruktur.

Client-Computer
Ein Computer auf der Client-Seite des Programms.

Ein Computer, auf dem der ePolicy Orchestrator-Agent installiert ist.

Client-Tasks
Auf Client-Computern ausgeführte Tasks.

Computer
Die physischen Computer im Netzwerk.

DAT-Dateien
Virusdefinitionsdateien, mit denen die Virenschutz-Software Viren und potenziell unerwünschten Code, der in Dateien eingebettet ist, erkennen kann.

Siehe auch EXTRA.DAT-Datei, Inkrementelle dat-Dateien und Superdat.

Denial of Service Attack
Eine Art von Angriff oder Eindringen bei einem Computer, Server oder Netzwerk, der die Möglichkeit, auf legitime Verbindungsanforderungen zu antworten, stört. Eine Denial of Service Attack überlastet das Ziel mit falschen Verbindungsanforderungen, so dass das Ziel legitime Anforderungen ignoriert.

Detailbereich
Der rechte Bereich der Konsole, der Details des aktuell ausgewählten Konsolenstrukturelement anzeigt. Je nach ausgewähltem Konsolenstrukturelements kann der Detailbereich in obere und untere Bereiche aufgeteilt sein.

Siehe auch Oberer Detailbereich und Unterer Detailbereich.

Direktionales Scannen
Scannen, bei der eine Appliance dem Eingehendes Scannen und eine andere Appliance dem Ausgehendes Scannen gewidmet ist.

Download-Site
Ein Repository, aus dem Sie Produkt- oder DAT-Aktualisierungen abrufen.

Siehe auch Update-Standort.

Echtzeit-Scannen
Siehe Scannen bei Zugriff.

EICAR
Das European Institute of Computer Anti-Virus Research hat eine Zeichenfolge entwickelt, die verwendet werden kann, um die richtige Installation und den richtigen Betrieb von Antivirus-Software zu testen.

Eigenschaften
Eigenschaften sind Attribute oder Charakteristiken eines Objekts, die verwendet werden, um seinen Status, sein Erscheinungsbild oder seinen Wert zu definieren.

Eingehendes Scannen
Vergleiche Ausgehendes Scannen.

Element
Siehe Konsolenstrukturelemente.

ePolicy Orchestrator-Agent
Eine intelligente Verknüpfung zwischen dem ePolicy Orchestrator-Server und den Virenschutz- und Sicherheitsprodukten. Der ePolicy Orchestrator-Agent erzwingt Richtlinien und Tasks auf Client-Computern, sammelt Daten und erstellt Berichte darüber, installiert Produkte, erzwingt Richtlinien und Tasks und sendet Ereignisse zurück an den Policy Orchestrator-Server.

ePolicy Orchestrator-Konsole
Eine Ansicht aller Virusaktivitäten und des Status, mit der Möglichkeit, Agenten und Produkte zu verwalten und bereitzustellen. Sie bietet die Möglichkeit, Antivirus- und Sicherheitsrichtlinien festzulegen und bei allen Agenten auf Client-Computern oder ausgewählten Computern durchzusetzen, sowie eine Task-Planungsfunktion, die sich an bestimmte Computer oder Gruppen mit geplanten Tasks und Richtlinien richtet, und ermöglicht die Ansicht und Anpassung von Berichten, um die Ausbringung, Virusausbrüche und aktuelle Schutzstufen zu kontrollieren.

ePolicy Orchestrator-Server
Ein Repository für alle Daten, die von verteilten ePolicy Orchestrator-Agenten gesammelt werden. Er enthält eine Datenbank, die Daten über den Produkteinsatz auf Client-Computern im Netzwerk sammelt, ein Berichterstellungs-Modul für die Kontrolle der Virusschutzleistung in Ihrem Unternehmen und ein Software-Repository, dass Produkte und Produktaktualisierungen für die Bereitstellung in Ihrem Netzwerk speichert.

Ereignisse
Von unterstützten Produkten erzeugt, identifizieren Ereignisse Aktivitäten auf Client-Computern – von Dienstereignisse bis zu Infizierungserkennungs-Ereignissen. Jedem Ereignis wird eine Gewichtung von "informativ" bis zu "kritisch" zugewiesen. Ereignisse und Eigenschaften ergeben die Daten, die in Berichten und Abfragen angezeigt werden.

Ergänzende Virusdefinitionsdatei
Siehe EXTRA.DAT-Datei.

EXTRA.DAT-Datei
Ergänzende Virusdefinitionsdatei, die als Reaktion auf einen Ausbruch eines neuen Virus oder einer neuen Variante eines bestehenden Virus erstellt wird.

Siehe auch DAT-Dateien, Inkrementelle dat-Dateien und Superdat.

Firewall
Ein Programm, das als Filter zwischen Ihrem Computer und dem Netzwerk oder dem Internet fungiert. Es scannt den Datenverkehr, der an Ihrem Computer eintrifft (Eingangsverkehr), und den, der von Ihrem Computer gesendet wird (Ausgangsverkehr). Er scannt den Verkehr auf Paketebene und blockiert ihn entweder oder lässt ihn zu, je nach den von Ihnen eingestellten Regeln.

FRAMEPKG.EXE
Das Agenten-Installationspaket. Wenn es ausgeführt wird, installiert diese Datei den ePolicy Orchestrator-Agenten auf einem Client-Computer.

Gemeinsames Framework
Eine Architektur mit Common-Core-Technologie, die es ermöglicht, dass verschiedene McAfee Security-Produkte dieselben gemeinsamen Komponenten und denselben gemeinsamen Code verwenden. Die Architektur dafür wird als gemeinsames Framework bezeichnet. Die Komponenten Planer, AutoUpdate und ePolicy Orchestrator-Agent sind gemeinsame Komponenten, die zum gemeinsamen Framework gehören.

Globale Aktualisierung
Eine Methode für die Bereitstellung von Produktaktualisierungen, sobald die entsprechenden Pakete in das Master-Repository eingecheckt wurden. Die Pakete werden sofort für alle SuperAgent- und globalen verteilten Repositories repliziert und der ePolicy Orchestrator-Server sendet eine Reaktivierung an alle SuperAgents; die SuperAgents senden eine Broadcastreaktivierung an alle Agenten im selben Subnet; anschließend rufen alle Agenten die Aktualisierung vom nächstgelegenen Repository ab.

Globale Berichtseinstellungen
Berichtseinstellungen, die alle ePolicy Orchestrator-Datenbankserver, -Berichte und -Abfragen betreffen.

Globaler Administrator
Ein Benutzerkonto mit Lese-, Schreib- und Löschberechtigungen sowie Rechten für alle Vorgänge. Vorgänge, die die gesamte Installation betreffen, können nur von den Benutzerkonten des globalen Administrators verwendet werden.

Vergleiche Standortadministrator und Globaler Prüfer.

Globaler Prüfer
Ein Benutzerkonto mit Leseberechtigungen; der globale Prüfer kann alle Einstellungen in der Software anzeigen, er kann jedoch keine dieser Einstellungen ändern.

Vergleiche Standortprüfer und Globaler Administrator.

Globales verteiltes Repository
Eine exakte Kopie der Pakete im Master-Repository.

Gruppe
In der Konsolenstruktur eine logische Sammlung von Entitäten, die zur leichteren Verwaltung zusammengefasst wurden. Gruppen können andere Gruppen oder Computer enthalten. Sie können IP-Adressbereiche oder-IP-Teilnetzmasken zu Gruppen zuordnen, um Computer nach IP-Adressen zu sortieren. Wenn Sie eine Gruppe durch Importieren einer Windows NT-Domäne erstellen, können Sie das Agenten-Installationspaket automatisch an alle importierten Computer in der Domäne senden.

Heuristische Analyse, Heuristik
Eine Scan-Methode, die nach Mustern oder Aktivitäten sucht, die virusähnlich sind, um neue oder bisher nicht erkannte Viren festzustellen.

Hintergrund-Scannen
Eine Art des Scannens bei Zugriff, ermöglicht durch Microsoft VS API2, bei der nicht alle Dateien beim Zugriff gescannt werden, so dass die Belastung des Scanners im Betrieb reduziert wird. Es werden Datenbanken gescannt, für die die Funktion aktiviert wurde, z. B. Mailbox-Store und Public Folder-Store.

Host, Host-Computer
Siehe Client-Computer.

Häufigkeit
Das sich wiederholende Intervall, für das der Task geplant werden soll.

Inaktiver Agent
Ein Agent, der für eine bestimmte Zeitspanne nicht mit dem ePolicy Orchestrator-Server kommuniziert hat.

Inkrementelle DAT-Dateien
Neue Virendefinitionen, die die derzeit installierten Virendefinitionen ergänzen. Sie ermöglichen es, dass das Aktualisierungs-Dienstprogramm nur die neuesten DAT-Dateien und nicht den gesamten Satz an DAT-Dateien herunterladen muss.

Siehe auch DAT-Dateien, EXTRA.DAT-Datei und Superdat.

Inkrementelle Replizierung
Vergleiche Vollständige Replizierung.

Installation erzwingen, Deinstallation erzwingen
Siehe Produktbereitstellungs-Client-Task++.

Knoten
Siehe Konsolenstrukturelemente.

Konsolenstruktur
Der linke Bereich der Konsole, der alle Konsolenstrukturelemente enthält.

Konsolenstrukturelemente
Jedes Element in der Konsolenstruktur.

Lokales verteiltes Repository
Speicherorte, die nur vom Client-Computer aus aufgerufen werden können; beispielsweise ein zugeordnetes Laufwerk oder ein FTP-Server, dessen Adresse nur über einen lokalen DNS-Server aufgelöst werden kann. Lokale verteilte Repositories sind in der Agentenrichtlinie für ausgewählte Client-Computer definiert.

Lost&Found-Gruppe
Ein Speicherort auf dem ePolicy Orchestrator-Server für Computer, deren geeigneter Speicherort im **Verzeichnis** nicht bestimmt werden kann. Der Server verwendet die IP-Verwaltungseinstellungen, Computernamen, Domänennamen und Standort- oder Gruppennamen, um die Platzierung der Computer zu bestimmen. Nur globale Administratoren haben vollen Zugriff auf die globale **Lost&Found**-Gruppe. Standortadministratoren können nur auf **Lost&Found**-Gruppen in den Standorten zugreifen, für die sie Zugriffsrechte besitzen.

Makrovirus
Ein bösartiges Makro – ein gespeicherter Satz an Anweisungen, erstellt, um Vorgänge innerhalb bestimmter Anwendungen oder Systeme zu automatisieren – das versehentlich ausgeführt werden kann und Schaden verursacht oder sich selbst repliziert.

Master-Repository
Der ePolicy Orchestrator-Server; auf ihm befindet sich eine Originalkopie der Pakete im Quell-Repository; er kann Pakete für verteilte Repositories replizieren. Auf der Ebene des Master-Repository können Sie Produkt- und Produktaktualisierungspakte einchecken, Tasks zur Replizierung von Paketen für globale verteilte Repositories oder über SuperAgent verteilte Repositories planen und Tasks für das Abrufen von Pakten aus Quell- oder Alternativ-Repositories und ihre Integration in das Master-Repository planen.

McAfee AutoUpdate Architect
McAfee Security-Software, die mit ePolicy Orchestrator zusammenarbeitet, um Produkte und Produktaktualisierungen in einem Unternehmen bereitzustellen.

Oberer Detailbereich
Der obere Abschnitt des Detailbereichs in der Konsole, der die Registerkarten **Richtlinien**, **Eigenschaften** und **Tasks** enthält.

Siehe auch Detailbereich und Unterer Detailbereich.

Paket
Enthält Binärdateien, Erkennungs- und Installationsskripts sowie eine Paketkatalogdatei (PKGCATALOG.Z), die für die Installation von Produkten und Produktaktualisierungen verwendet wird.

Paketkatalogdatei
Eine Datei (PKGCATALOG.Z), die Einzelheiten zu den einzelnen Aktualisierungspaketen enthält, unter anderem den Namen des Produkts, für das die Aktualisierung gedacht ist, die Sprachversion und etwaige Installationsabhängigkeiten.

Paketsignierung, Paketsicherheit
Ein System zur Signaturprüfung zur Sicherung der von Network Associates erstellten und verteilten Pakete. Die Pakete werden mit einem Schlüsselpaar unter Verwendung des Signaturprüfungssystems DSA (Digital Signature Algorithm) mit einer 168-Bit-3DES-Verschlüsselung verschlüsselt. Schlüssel werden zur Ver- bzw. Entschlüsselung vertraulicher Daten verwendet.

Produktbereitstellungs-Client-Task++
Ein geplanter Task zur Bereitstellung aller Produkte, die derzeit gleichzeitig im Master-Repository eingecheckt sind. Dieser Task ermöglicht die Planung der Produktinstallation und -entfernung außerhalb der Stoßzeiten oder während des Richtlinienumsetzungsintervalls.

Protokoll
Eine Aufzeichnung der Aktivitäten einer Komponente der McAfee-Antiviren-Software. Protokolle zeichnen die Aktionen bei einer Installation oder während Scan- und Aktualisierungs-Tasks auf.

Siehe auch Ereignisse.

Pull-Task
Siehe Repository-Pull-Server-Task.

Quarantäne
Durchgesetzte Isolierung einer Datei oder eines Ordners, um eine Virusinfizierung zu verhindern. VirusScan Enterprise stellt infizierte Dateien oder Ordner unter Quarantäne, bis das Element gesäubert oder entfernt werden kann.

Quell-Repository
Ein Speicherort, von dem ein Master-Repository Pakete abruft.

Remote-Konsole
Die Konsole läuft auf einem Computer, auf dem der ePolicy Orchestrator-Server nicht läuft. Remote-Konsolen ermöglichen mehreren Personen den Zugriff auf den Server, um Aktionen zu prüfen oder Standorte und Installationen zu verwalten.

Siehe auch ePolicy Orchestrator-Konsole.

Replizierungs-Task
Siehe Repository-Replizierungs-Server-Task.

Repository
Der Speicherort, an dem Richtlinienseiten für die Verwaltung von Produkten gespeichert werden.

Repository-Liste
Die Datei SITELIST.XML, die von den McAfee-Antiviren-Produkten, die AutoUpdate 7.0 verwenden, zum Zugriff auf verteilte Repositories und zum Abrufen von Paketen aus diesen Repositories verwendet wird.

Repository-Pull-Server-Task
Ein Task, der das Quell- oder Alternativ-Repository angibt, aus dem die Pakete abgerufen und anschließend in die angegebenen Unterebenen im Master-Repository integriert werden sollen.

Repository-Replizierungs-Server-Task
Ein Task für die Aktualisierung globaler verteilter Repositories und über SuperAgent verteilte Repositories zur Aufrechterhaltung identischer Kopien aller Pakete auf allen Unterebenen im Master-Repository. Sie haben auch die Möglichkeit, ausgewählte verteilte Repositories zu aktualisieren.

Richtlinie
Konfigurationseinstellungen für jedes Produkt, die über ePolicy Orchestrator verwaltet werden können und festlegen, wie sich das Produkt auf Client-Computern verhält.

Vergleiche Task. Siehe auch Agentenrichtlinien.

Richtlinienseiten
Als Teil der ePolicy Orchestrator-Konsole ermöglichen Sie Ihnen, Richtlinien festzulegen und geplante Tasks für Produkte zu erstellen, und werden auf einzelnen ePolicy Orchestrator-Servern gespeichert (sie werden nicht dem Master-Repository hinzugefügt).

Richtlinienumsetzungsintervall

Bestimmt, wie oft der Agent die Richtlinien umsetzt, die er vom ePolicy Orchestrator-Server erhalten hat. Da Richtlinien lokal durchgesetzt werden, wird für dieses Intervall keine Bandbreite benötigt.

Richtlinienvererbung

Legt fest, ob die Richtlinieneinstellungen, die für irgendein Element in der Konsolenstruktur unter dem **Verzeichnis** geplant sind, aus dem unmittelbar darüber liegenden Element entnommen werden.

Scannen

Eine Überprüfung von Dateien, um festzustellen, ob ein Virus oder ein potenziell unerwünschter Code vorliegt.

Siehe Scannen bei Zugriff und Scannen auf Anforderung.

Scannen auf Anforderung

Eine geplante Überprüfung ausgewählter Dateien, um festzustellen, ob ein Virus oder ein potenziell unerwünschter Code vorliegt. Diese Prüfung kann sofort durchgeführt werden, zu einem geplanten Zeitpunkt in der Zukunft oder in regelmäßigen geplanten Zeitintervallen.

Vergleiche Scannen bei Zugriff.

Scannen bei Zugriff

Eine Prüfung in Verwendung befindlicher Dateien, um festzustellen, ob sie einen Virus oder potenziell unerwünschten Code enthalten. Diese Prüfung kann immer dann erfolgen, wenn eine Datei vom Datenträger gelesen und/oder auf den Datenträger geschrieben wird.

Vergleiche Scannen auf Anforderung.

Scan-Aktion

Die Aktion, die stattfindet, wenn eine infizierte Datei gefunden wird.

Scherzprogramm

Ein sich nicht replizierendes Programm, das einen Endbenutzer warnt oder stört, aber an Dateien oder Daten keinen tatsächlichen Schaden verursacht.

Selektive Aktualisierung

Die Angabe, welche Aktualisierungsversion (**Test**, **Aktuell** oder **Früher**) die Client-Computer abrufen sollen.

Server-Tasks

Tasks, die der Server zu Wartungszwecken in der ePolicy Orchestrator-Datenbank und im **Repository** durchführt. Zu den standardmäßigen Server-Tasks gehören **Wartung inaktiver Agenten**, **Repository-Pull**, **Repository-Replizierung** und **Domänen synchronisieren**.

Spam-E-Mail, Spam-Nachricht

Jede unerwünschte und unwillkommene E-Mail-Nachricht, einschließlich kommerzieller E-Mails. Das elektronische Äquivalent von Postwurfsendungen sowie unerwünschte nicht kommerzielle E-Mail-Nachrichten wie z. B. Virus-Hoaxe, Scherzprogramme und Kettenbriefe.

Spiegelungstask
Tasks, mit denen der Inhalt des ersten Repository in der Repository-Liste in das von Ihnen angegebene Verzeichnis auf dem Client-Computer kopiert wird.

SPIPE
Secured PIPE, ein gesichertes Kommunikationsprotokoll, das ePolicy Orchestrator-Server verwenden.

Standardvorgang
Jeder Vorgang in VirusScan Enterprise, der nicht als Vorgang mit geringem Risiko oder Vorgang mit hohem Risiko definiert ist.

Siehe auch Vorgang mit hohem Risiko und Vorgang mit geringem Risiko.

Standort
In der Konsolenstruktur eine logische Sammlung von Entitäten, die zur leichteren Verwaltung zusammengefasst wurden. Standorte können Gruppen oder Computer enthalten und nach IP-Adressbereich, IP-Subnet-Maske, Speicherort, Abteilung usw. organisiert sein.

Standortadministrator
Ein Benutzerkonto mit Lese-, Schreib- und Löschberechtigungen sowie Rechten für alle Vorgänge (außer denjenigen, die auf den globalen Administrator beschränkt sind) auf dem angegebenen Standort und allen Gruppen und Computern, die sich unter diesem Standort in der Konsolenstruktur befinden.

Vergleiche Globaler Administrator und Standortprüfer.

Standortprüfer
Ein Benutzerkonto mit Leseberechtigungen; der Standortprüfer kann dieselben Einstellungen anzeigen wie der Standortadministrator, er kann jedoch keine dieser Einstellungen ändern.

Vergleiche Globaler Prüfer und Standortadministrator.

SuperAgent
Ein Agent mit der Fähigkeit, mithilfe der SuperAgent-Reaktivierung Kontakt mit allen Agenten im selben Subnet wie der SuperAgent aufzunehmen. Er wird für die globale Aktualisierung verwendet und unterstützt verteilte Software-Repositories, wodurch die Notwendigkeit eines dedizierten Servers entfällt. Er bietet eine bandbreiteneffiziente Methode zum Senden von Agenten-Reaktivierung.

Siehe auch ePolicy Orchestrator-Agent.

SuperAgent-Reaktivierung
Ein geplanter Task oder Anforderungsbefehl, der SuperAgents (und alle Agenten im selben Subnet wie die einzelnen SuperAgents) auffordert, bei Bedarf Kontakt mit dem ePolicy Orchestrator-Server aufzunehmen, anstatt auf den nächsten ASCI-Befehl zu warten.

Siehe auch Agentenreaktivierung.

SuperDAT
Ein Dienstprogramm, das aktualisierte Virusdefinitionsdateien (SDAT*.EXE) installiert und bei Bedarf das Scan-Modul aktualisiert.

Siehe auch DAT-Dateien, EXTRA.DAT-Datei und Inkrementelle dat-Dateien.

Systemscan
Der Scan eines festgelegten Systems.

Task
Eine Aktivität (sowohl einmalige Aktivitäten, wie Scannen auf Anforderung, als auch Routineaktivitäten, wie Aktualisierung), die so geplant sind, dass sie zu einem bestimmten Zeitpunkt oder in bestimmten Intervallen ausgeführt werden.

Vergleiche Richtlinie.

Task-Vererbung
Legt fest, ob die Client-Tasks, die für irgendein Element in der Konsolenstruktur unter dem **Verzeichnis** geplant sind, aus dem unmittelbar darüber liegenden Element entnommen werden.

Trojanisches Pferd
Ein Programm, das entweder vorgibt, nützliche oder erwünschte Funktionen zu bieten oder so beschrieben wird, aber tatsächlich eine schädliche Wirkung in sich birgt. Trojanische Pferde sind technisch gesehen keine Viren, da sie sich nicht replizieren.

Unterer Detailbereich
Der untere Abschnitt des Detailbereichs in der Konsole, der die Konfigurationseinstellungen für die aufgelisteten Produkte in der Registerkarte **Richtlinien** im oberen Detailbereich anzeigt.

Siehe auch Detailbereich und Oberer Detailbereich.

Update-Standort
Das Repository, aus dem Sie Produkt- oder DAT-Aktualisierungen abrufen.

Siehe auch Download-Site.

UTC-Zeit
Universal Time Coordinated (UTC). Die Zeit auf dem 0-Meridian (Greenwich).

Über Spiegel verteiltes Repository
Ein lokales Verzeichnis auf Client-Computern, deren Replizierung mithilfe eines **Spiegelungs**-Client-Tasks erfolgt und von dem andere Client-Computer Aktualisierungen abrufen können.

Über SuperAgent verteiltes Repository
Eine Replizierung des Master-Repository, die anstelle von dedizierten Servern für globale verteilte Repositories verwendet wird.

Vererbung
Siehe Task-Vererbung und Richtlinienvererbung.

Verpackte Programmdatei
Eine verpackte Programmdatei ist eine Datei, die sich beim Ausführen nur direkt in den Speicher extrahiert. Verpackte Programmdateien werden nie auf Festplatte extrahiert.

Verteiltes Software-Repository
Architektur für die Bereitstellung von Produkten und Produktaktualisierungen in einem Unternehmen. Sie erstellt eine zentrale Bibliothek unterstützter Produkte und Produktaktualisierungen im Master-Repository.

Verzeichnis
Listet alle Computer auf, die über ePolicy Orchestrator zu verwalten sind, und stellt die Verknüpfung zu den Hauptbenutzeroberflächen für die Verwaltung dieser Computer dar.

Virus
Ein Programm, das in der Lage ist, sich mit keiner oder geringer Benutzerintervention zu replizieren. Die replizierten Programme replizieren sich wiederum.

Virusdefinitionsdateien (DAT)
Siehe DAT-Dateien.

VirusScan Enterprise-Konsole
Die Steuerungszentrale für die Aktivitäten des Programms.

Virus-Scan-Modul
Der Mechanismus, der den Scan-Vorgang antreibt.

Vollständige Replizierung
Vergleiche Inkrementelle Replizierung.

Vorgang mit geringem Risiko
In VirusScan Enterprise sind das Vorgänge, die McAfee Security mit geringerer Wahrscheinlichkeit als infiziert einstuft. Zum Beispiel:

Backup-Software

Code-Compiler/Linker-Prozesse.

Siehe auch Standardvorgang und Vorgang mit geringem Risiko.

Vorgang mit hohem Risiko
In VirusScan Enterprise sind das Vorgänge, die McAfee Security mit größerer Wahrscheinlichkeit als infiziert einstuft. Zum Beispiel:

Vorgänge, die andere Vorgänge auslösen, beispielsweise Microsoft Windows-Explorer oder die Eingabeaufforderung.

Vorgänge für die Ausführung, beispielsweise WINWORD oder CSCRIPT.

Vorgänge für das Herunterladen aus dem Internet, beispielsweise Browser, Instant Messenger und Mail-Clients.

Siehe auch Standardvorgang und Vorgang mit geringem Risiko.

Warnpriorität
Der Wert, den Sie jeder Warnmeldung zu Informationszwecken zuweisen. Warnmeldungen können folgende Prioritäten zugewiesen werden: kritisch, hoch, Warnung, informativ.

Warnung
Eine Meldung oder Benachrichtigung über Computeraktivitäten, beispielsweise Virenerkennung. Sie kann automatisch gemäß einer vordefinitierten Konfiguration per E-Mail, Pager oder Telefon an Systemadministratoren und Benutzer gesendet werden.

Worm (Wurm)
Ein Virus, der sich durch Erstellung von eigenen Duplikaten auf anderen Laufwerken, Systemen oder Netzwerken verbreitet.

Zentrale Warnungen
Eine Alternative zur Verwendung des regulären Warnungs-Managers. Durch Virenschutz-Software (z. B. VirusScan Enterprise 7.0) erzeugte Warnmeldungen werden in einem freigegebenen Ordner auf einem Server gespeichert. Der Warnungs-Manager wird für das Lesen von Warnbenachrichtigungen aus diesem Ordner konfiguriert. Wenn sich der Inhalt des freigegebenen Ordners ändert, werden vom Warnungs-Manager neue Warnbenachrichtigungen gesendet. Dabei werden die Warnmethoden verwendet, für die der Warnungs-Manager bereits konfiguriert ist. E-Mail-Nachrichten könnten z. B. an einen Pager gesendet werden.

Zufallsgenerierung
Ein zufälliger Punkt innerhalb eines Zeitintervalls, das Sie für einen geplanten Task festgelegt haben.

Index

A

Abschneiden von Warnmeldungen, erzwingen, 181
Aktivieren der Zufallsgenerierung, 242
Aktivitätsprotokoll für
  AutoUpdate-Task, 210
  E-Mail-Empfangsscan, 144
  E-Mail-Scan auf Anforderung, 160
  Scannen auf Anforderung, 121
  Scannen bei Zugriff, 88
  Spiegelungstask, 230
Aktualisieren
  Aktivitäten, 209
  Download-Sites, 211
    FTP, Standard-Download-Site, 211, 217, 232
    HTTP, Standard-Download-Site, 211, 217
  Fehlercodes, 284
  manuell, 232
  Proxy-Einstellungen, 221
  Repository-Liste, 210
    Repositories bearbeiten, 213
    Repositories entfernen und neu organisieren, 220
  Spiegelungstask, 226
  Strategien, 200
  Tasks
    ausführen
      fortsetzbare Aktualisierung, 206
      sofortige Aktualisierung, 206
    konfigurieren, 204
Allgemeine Einstellungen, Eigenschaften, beim Scannen bei Zugriff, 49
Allgemeine Fragen, Fehlerbehebung, 281
Angeben von Dateityperweiterungen (mit dem Feature "Angegebene"), 76
Anzeigeoptionen, 33
Archivdateien, Scannen, 263
Argumente, für Anforderungsscanner anwendbar, 262
Ausschließen von Dateien, Ordnern und Laufwerken (mit dem Feature "Ausschlüsse"), 78
Automatisches Scannen, 39
AutoUpdate
  Aktivitätsprotokoll anzeigen, 210
  Beschreibung, 202
  Download-Sites, 211
    FTP, Standard-Download-Site, 211, 217, 232
    HTTP, Standard-Download-Site, 211, 217
  Fehlercodes, 284
  implementieren (*Siehe* Aktualisieren mit dem VirusScan Enterprise-Implementierungshandbuch)
  Proxy-Einstellungen, 221
  Repository-Liste, 210
    Repositories bearbeiten, 213
    Repositories entfernen und neu organisieren, 220
    Repositories hinzufügen, 213
    Repositories importieren, 212
  Tasks
    Aktivitäten während der Aktualisierung, 209
    ausführen, 206
      fortsetzbare Aktualisierung, 206
      mithilfe des Menüs "Start", 208
      mithilfe von "Jetzt aktualisieren", 208
      sofortige Aktualisierung, 206
      über die Konsole, 207
    erstellen, 204
    konfigurieren, 204
    planen, 207
    Übersicht über den Aktualisierungsvorgang, 203
AVERT (Anti-Virus Emergency Response Team), Kontaktaufnahme, 12

B

Befehlszeile, Windows, 32
  Anforderungsscanner ausführen von, 262
  Optionen, 253
Begrenzen der Protokolldateigröße, 54, 114, 141, 157
Benutzername, Aufzeichnung in Protokolldatei, 55, 115, 142, 158
Benutzeroberfläche
  Optionen
    Anzeige, 33
    entsperren, 37
    festlegen, 32
    Kennwort, 34
    sperren, 37
  Orientierung, 22
Berichtseigenschaften konfigurieren
  E-Mail-Empfangsscan, 140
Berichtseigenschaften, Konfigurieren
  E-Mail-Scan auf Anforderung, 156
  Scannen auf Anforderung, 113
  Scannen bei Zugriff, 53
Beta-Programm, Kontaktaufnahme, 12
Boot-Sektoren
  mit Anforderungsscanner scannen, 101
  mit Zugriffsscanner scannen, 50
  Scannen von der Befehlszeile aus, 255

C

CAB, Scannen von Dateien mit der Erweiterung, 263
CATALOG.Z (Datei), 209

D

DAT-Dateiaktualisierungen, Website, 12
DAT-Dateien
  Rollback durchführen, 230
Dateityperweiterungen, zu scannende Elemente
  Ausschließen von Dateitypen (mit dem Feature "Ausschlüsse"), 78
  Hinzufügen benutzerdefinierter Typen (mit dem Feature "Angegebene"), 76
  Hinzufügen von Dateitypen (mit dem Feature "Ergänzungen"), 75
Datum und Uhrzeit, Aufzeichnung in Protokolldatei, 55, 115, 142, 158
Definition der Begriffe (*Siehe* Glossar)
Disketten beim Herunterfahren
  mit Zugriffsscanner scannen, 50
Dokumentation zum Produkt, 11
Download-Website, 12

E

Eigenschaften des Warnungs-Managers
  Zusammenfassung, 170
E-Mail, Senden von Virenwarnungen, 177
E-Mail-Scan, auf Anforderung
  Aktivitätsprotokoll anzeigen, 160
  Tasks ausführen, 158
  Tasks konfigurieren, 145
    Aktionseigenschaften, 151
    Berichtseigenschaften, 156
    Erkennungseigenschaften, 145
    erweiterte Eigenschaften, 148
    Warnungseigenschaften, 154
E-Mail-Scan, bei Empfang
  Aktivitätsprotokoll anzeigen, 144
  Scan-Statistiken, Anzeigen, 142
  Tasks konfigurieren, 128
    Aktionseigenschaften, 135
    Berichtseigenschaften, 140
    Erkennungseigenschaften, 129
    erweiterte Eigenschaften, 131
    Warnungseigenschaften, 138
Entsperren der Benutzeroberfläche, 37
Erkennung von Viren
  Scannen auf Anforderung
    Aktionen durchführen, 123
    Empfangen von Benachrichtungen, 122
  Scannen bei Zugriff
    Aktionen durchführen, 92
    Empfangen von Benachrichtungen, 89
    Meldungen anzeigen, 91
Erste Schritte, 21
EXTRA.DAT, 199, 209

F

FAQ (Häufig gestellte Fragen), 277
Features, Beschreibung, 17
Fehlerbehebung, 277
  Fehlercodes aktualisieren, 284
  häufig gestellte Fragen
    Allgemein, 281
    Installation, 278
    Scannen, 279
    Viren, 279
  Minimum Escalation Tool, 277
Fortsetzbare Scan-Vorgänge, 119
Fragen zur Installation, Fehlerbehebung, 278
FTP, Standard-Download-Site, 211, 217, 232

H

Handbücher, 11
Häufig gestellte Fragen (FAQ), 277
Herstellen einer Verbindung zu Remote-Servern, 42
Hinzufügen von Dateityperweiterungen (mit dem Feature "Ergänzungen"), 75
HTTP, Standard-Download-Site, 211, 217

I

Informationsquellen, 11
Installation (*Siehe* Installationshandbuch)

J

Jetzt aktualisieren (Befehl), 208
Jetzt spiegeln (Befehl), 229

K

Kennwortoptionen, 34
KnowledgeBase-Suche, 12
Komprimierte Dateien
  Scannen von der Befehlszeile aus
    Archivtyp, 263
Konfigurieren
  E-Mail-Empfangsscan, 128
  E-Mail-Scan auf Anforderung, 145
  Scannen auf Anforderung, 96
  Scannen bei Zugriff, 45
  Spiegelungstask, 225
  über ePolicy Orchestrator (*Siehe* Konfigurationshandbuch)
konfigurieren
  AutoUpdate-Task, 204
Konsole (*siehe* VirusScan-Konsole)
Kontaktaufnahme mit McAfee Security, 12
Kontextmenüs, 28
Konventionen in diesem Handbuch, 10
Kundendienst, Kontaktaufnahme, 12

L

Liste der Tasks in der VirusScan-Konsole, 27
LZH, Scannen von Dateien mit der Erweiterung, 263

M

Mail-Server, für das Senden von Warnungen per E-Mail konfigurieren, 179
McAfee Security University, Kontaktaufnahme, 12
Meldungen, Scannen bei Zugriff, 51
  anzeigen, 91
  Anzeigen von Meldungen, Dialogfeld, 52
  anzuzeigender Text, 52
  infizierte Dateien bereinigen, auf die verwiesen wird, 52
  infizierte Dateien löschen, auf die verwiesen wird, 52
  infizierte Dateien verschieben, auf die verwiesen wird, 52
  Nachricht an Benutzer senden, 52
  Nachrichten aus Liste entfernen, 52
  Remote-Benutzer trennen, 53
  Zugriff auf freigegebenes Netzwerkverzeichnis verweigern, 53

Menü "Ansicht", 25
Menü "Bearbeiten", 25
Menü "Extras", 25
Menü "Hilfe", 25
Menü "Task", 24
Menüleiste, 24
Menüs
Start, 22
VirusScan-Konsole, 24
Ansicht, 25
bearbeiten, 25
Extras, 25
Hilfe, 25
Kontextmenüs, 29
Task, 24
MERTool (Minimum Escalation Tool), 277
Minimum Escalation Tool (MERTool), 277

N

Netzwerkmeldungen übertragen, 175
Neue Funktionen, 16
Neustart von Anforderungstasks, 119

O

Ordner für Warnungen
Funktion, 190

P

Planen, 235
erweiterte Optionen, 240
Task-Eigenschaften, 237
Tasks, 236
AutoUpdate, 207
bei der Anmeldung, 249
bei Leerlauf, 250
bei Systemstart, 248
einmal, 246
für Ausführung beim Einwählen, 252
für sofortige Ausführung, 251
monatlich, 244
Scannen auf Anforderung, 116
spiegeln, 228
täglich, 241
wöchentlich, 243
Zeitplan-Eigenschaften, 238
Häufigkeit, 239
Zufallsgenerierung aktivieren, 242
PrimeSupport, 12
Priorisieren der gesendeten Nachrichten
an andere Computer, 169
im Netzwerk, 175, 177, 180, 183 bis 184, 186, 188, 190
Prioritätsstufe, für Warnungen einrichten, 169
Produktdokumentation, 11
Produktfeatures, 17
Produktschulungen, Kontaktaufnahme, 12
Protokolldatei für
AutoUpdate-Task, 210
E-Mail-Empfangsscan, 144
E-Mail-Scan auf Anforderung, 160
Scannen auf Anforderung, 121
Scannen bei Zugriff, 88
Spiegelungstask, 230
Protokolldatei, Größe
begrenzen, 54, 114, 141, 157
Proxy-Einstellungen für die Aktualisierung, 221

Q

Quarantäneordner
E-Mail-Empfangsscan, 136
E-Mail-Scan auf Anforderung, 153
Scannen auf Anforderung, 111
Scannen bei Zugriff, 50

R

Rechte Maustaste, Scannen, 30
über die Systemablage, 30
Registrierung sperren, 269 bis 276
Registrierung, sichere, 269 bis 276
Remote-Verbindung, im Menü "Extras", 42
Remoteverwaltung, 42
Repositories, 220
Repository-Liste
Repositories bearbeiten, 213
Repositories entfernen und neu organisieren, 220
Repositories hinzufügen, 213
Repositories importieren, 212

S

Scannen
- auf Anforderung, 96
- automatisch, 39
- bei Auswahl, 40
- bei Zugriff, 45
- bei Zugriff im Vergleich zum Scannen auf Anforderung, 38
- E-Mail auf Anforderung, 145
- E-Mail bei Empfang, 128
- Ergebnisse anzeigen
  - Aktivitätsprotokoll des E-Mail-Scans auf Anforderung, 160
  - Aktivitätsprotokoll des Spiegelungstasks, 230
  - AutoUpdate-Aktivitätsprotokoll, 210
  - E-Mail-Empfangsscan
    - Aktivitätsprotokoll, 144
    - Statistik, 142
  - Scannen auf Anforderung
    - Aktivitätsprotokoll, 121
    - Statistik, 120
  - Scannen bei Zugriff
    - Aktivitätsprotokoll, 88
    - Statistik, 87
- Fragen zur Fehlerbehebung, 279
- konfigurieren
  - Anforderungsscanner für, 96
  - E-Mail-Anforderungsscanner, 145
  - E-Mail-Empfangsscanner, 128
  - Zugriffsscanner, 45
- Rechte Maustaste, Scannen, 30
- rechte Maustaste, Scannen
  - über die Systemablage, 30
- regelmäßig, 40
- Shell-Erweiterungs-Scan, 30
- sofort, 117
- Vorgänge
  - automatisch, 39
  - bei Auswahl, 40
  - einrichten, 38
  - regelmäßig, 40
  - zu festgelegten Zeiten, 40
- zu festgelegten Zeiten, 40

Scannen (Menü)
- Statistik, 87, 89, 143 bis 144

Scannen auf Anforderung
- Aktivitätsprotokoll anzeigen, 121
- Scan-Statistiken, Anzeigen, 120
- Tasks
  - ausführen
    - beenden, 119
    - neu starten, 119
    - über die Konsole, 117
    - über die Windows-Befehlszeile, 262
    - unterbrechen, 119
  - erstellen, 96
    - mithilfe des Menüs "Start", 96
    - über die Konsole, 98
    - über die Systemablage, 96
  - Fortsetzbare Scan-Vorgänge, 119
  - konfigurieren, 99
    - Aktionseigenschaften, 110
    - Berichtseigenschaften, 113
    - Erkennungseigenschaften, 104
    - erweiterte Eigenschaften, 106
    - Ortseigenschaften, 100
  - planen, 116
- Viruserkennung, Antworten auf, 121

Scannen auf Anforderung im Vergleich zum Scannen bei Zugriff, 38

Scannen bei Zugriff
- Aktivitätsprotkoll anzeigen, 88
- konfigurieren, 46
  - Aktionseigenschaften, 64, 84
  - allgemeine Eigenschaften, 49
  - Benachrichtigungseigenschaften, 51
  - Berichtseigenschaften, 53
  - Erkennungseigenschaften, 59, 72
  - erweiterte Eigenschaften, 62, 81
  - Vorgangseigenschaften
    - geringes Risiko, 57, 67
    - hohes Risiko, 57, 67
    - Risiko zuweisen, 67
    - Standard, 57 bis 58
- Meldungen anzeigen, 91
- Scan-Statistiken anzeigen, 87
- Viruserkennung, Antworten auf, 89

Scannen bei Zugriff im Vergleich zum Scannen auf Anforderung, 38
Scannen zu festgelegten Zeiten, 40
Scan-Zeit
    Scannen bei Zugriff, 50
Schulungs-Website, 12
Service-Portal, PrimeSupport, 12
Sichere Registrierung, 269 bis 276
Sicherheitshauptquartier, Kontaktaufnahme mit AVERT, 12
Sitzungseinstellungen, Aufzeichnung in Protokolldatei, 55, 115, 142, 158
Sitzungszusammenfassung, Aufzeichnung in Protokolldatei, 55, 115, 142, 158
SMTP-Mail-Server, für das Senden von Warnungen per E-Mail konfigurieren, 179
SNMP
    Warnungen senden per, 183
Sperren der Benutzeroberfläche, 37
Spiegelungstask, 224
    Aktivitätsprotokoll anzeigen, 230
    ausführen, 228
        mithilfe des Befehls "Start", 229
        mithilfe von "Jetzt spiegeln", 229
        sofort, 229
        wie geplant, 228
    erstellen, 225
    konfigurieren, 226
    planen, 228
Standardvorgänge, 57 bis 58
Start, Scannen bei, 50
Startmenü, 22
Statistik, Anzeigen
    E-Mail-Empfangsscan, 142
    Scannen auf Anforderung, 120
    Scannen bei Zugriff, 87
Statistik, im Menü "Scannen", 87, 89, 143 bis 144
Statusleiste, 28
Symbolleiste, 26
Systemablage, Optionen festlegen, 30
Systemstart, Scannen bei, 50
Systemvariablen, 201
Systemvariablen, Warnungen, 196

T

Taskliste, 27
Tasks
    beenden, 119
    Definition von, 27
    Konfigurieren
        AutoUpdate-Task, 204
    konfigurieren
        Anforderungsscanner, 96
        E-Mail-Anforderungsscanner, 145
        E-Mail-Empfangsscanner, 128
        Spiegelungstask, 225
        Zugriffsscanner, 45
    neu starten, 119
    sofort ausführen, 117
    unterbrechen, 119
    verfügbare Typen in VirusScan Enterprise, 27
Technischer Support, 12 bis 13
Testen der Warnungskonfiguration, 168

U

Übermitteln eines Virusbeispiels, 12
Unterbrechen von Anforderungstasks, 119
Upgrade-Website, 12
UTC Coordinated Universal Time (UTC), 242
UUE, Scannen von Dateien mit der Erweiterung, 263

V

Variablen, System-, 201
Verbesserungen und neue Funktionen, 16
Viren
    Beispiel senden, 41
    Erkennung
        Scannen auf Anforderung, 121
        Scannen bei Zugriff, 89
    häufig gestellte Fragen, 279
Virus, Übermitteln eines Beispiels, 12
Virusinformationsbibliothek, 12, 41
VirusScan Enterprise
    Produktfeatures, 17
    Verbesserungen und neue Funktionen, 16

VirusScan-Konsole, 23
konfigurieren
AutoUpdate (*Siehe* AutoUpdate)
E-Mail-Empfangsscan (*siehe* E-Mail-Scan, bei Empfang)
E-Mail-Scan auf Anforderung (*siehe* E-Mail-Scan, auf Anforderung)
Scannen auf Anforderung (*siehe* Scannen auf Anforderung)
Scannen bei Zugriff (*Siehe* Scannen bei Zugriff)
Spiegelungstask (*Siehe* Spiegelungstask)
Menüs (*siehe* Menüs)
Statusleiste, 28
Symbolleiste, 26
Taskliste, 27
Verbindungen zu Remote-Servern herstellen, 42
Vorgänge mit geringem Risiko, 57, 67
Definition, 67
Vorgänge mit hohem Risiko, 57, 67
Definition, 68

W

Warnmeldungen
abschneiden, 181
aktivieren, 193
an Drucker senden, 181
anpassen, 192
bearbeiten, 196
deaktivieren, 193
E-Mails, 177
Netzwerkwarnungen übertragen, 175
Programm als Antwort starten, 185
über SNMP-Traps senden, 183
Variablen in, 197
weiterleiten, 171
zentrale Warnungen, 190
Warnmethode
Empfänger konfigurieren, 167
Warnungs-Manager
Konfiguration
E-Mail-Warnung, 177
gedruckte Meldungen, 181
Netzwerkübertragungen, 175
Programm starten, 185
SNMP, 183
Warnungen weiterleiten, 171
Systemvariablen, 196
Zusammenfassung (Seite), 170
Warnungspriorität
ändern, 194
Arten, 195
Weiterleiten von Warnungen
große Unternehmen, 172
kleine Unternehmen, 173

Z

Zentrale Warnungen, 190
Zielgruppe des Handbuchs, 9
ZIP, Scannen von Dateien mit der Erweiterung, 263